NO. 24 March 2012 • Price Free • www.networkset.net

NetWork Set

أهم خمس شهادات تقنية بحسب دراسة NetworkSet

Cron: automation of the commands

الشبكات الافتراضية.. أنواعها وتطبيقاتها

أوامر التحقق من عمل الشبكة

الـ Honeypot مصيدة للهاكرز

حلق في آفاق الوايرلس مع n 802.11

أيهم أفضل CCNP Sec أم CEH !!

Migration or update ? Is your choice

مقدمة عن سويتشات HP

شحذ الهمم (2)

أفكر فيما سأكتب وكيف أبدا ولكن ما أن جلست أمام ملف الوارد وبدأت أتخيل هذا الموضوع وجدت نفسي مباشرة ولا تسألوني لماذا أعود إلى الماضي إلى أيام الدراسة الأبتدائية والإعدادية وتحديدا إلى الأيام الاولى من كل عام دراسي وكيف كنت أبدا أولا أيامي وأنا مشتاق للمدرسة وللدراسة فتجدني أكتب وظائفي يوميا وأحفظ دروسي وأنهي واجباتي فور عودتي للبيت وأحيانا كنت أحاول قراءة وتجهيز الدروس القادمة والتى لم نحصل عليها بعد من المدرسة, هل مررت بهذا السيناريو من قبل ؟ لو كان جوابك بنعم فإذا وافقني الرائي بأن هذا النشاط النووي لم يكن يتجاوز الأسبوع أو الأسبوعان كحد أقصى وبعدها تعود الحياة إلى ماهي عليه, تقصير وعدم متابعة وكتابة الوظائف في المدرسة وملل وقرف وجملة متى سوف يحين الصيف وتغلق المدرسة.

هذا الأمر كنت دائما ما أفكر فيه مليا من خلال العودة بالذاكرة إلى تلك الأيام محاولا مناقشة ذلك السؤال مع نفسي وهو لماذا كنت أعيش هذه الحالة النشيطة والهمة العالية في البداية وبعدها يزول كل شيئ, الأسباب كثيرة لكن سوف أتعامل مع بعضها لتحديد أسباب إنخفاض الهمم وخصوصا أن تحدثت سابقا أن الهمم موجودة لكن هناك مايدفعها دوما للأسفل والحل هو بالتفكير بالمسببات وليس البحث عن الطرق لرفع الهمم, وبعد تناول الأفكار الرئيسية للجزء الثاني من المقال سوف أقدم تجربتي في هذا المجال.

النقطة الأولى التى سوف أناقشها معك هي أهمية العلم فالكثير ولا أعمم يعتبر العلم والدراسة هي وسيلة للحياة أو وسيلة للعمل فتجده يربط علمه وطريقة دراسته مع متطلبات العمل وهي الكارثة التى نقع فيها والتى تكون نتيجتها علم تجاري قد يخدمك قليلا على المستوى الشخصي لكن أن تكون مميزا ولك إسمك وشهرتك في مجالك لن تصل إليه مهما حاولت مستقبلا لذلك حرر عقلك من هذه النقطة وتعامل مع العلم ومع الدراسة كمادة علمية فقط .

النقطة الثانية وهي نقطة خطيرة وتزيل الهمم التى كالجبال وهي الأستعجال والرغبة في الوصول بشكل سريع, هذه النقطة توصلت إليها من خلال أشخاص دخلوا مدونتي وأعجبوا بها وبعد أيام حذفوها من مفضلتهم ولم يعودوا يدخلوا إليها, فعادة عندما يبدأ أي طالب علم ذو همة عالية الدراسة وطلب العلم يتوجه إلى الانترنت ويبدأ البحث عن مصادر جيدة فيجد الكثير من المواقع والمدونات ويبدأ يقرا من هنا ومن هناك ويفأجئ بالكم الهائل من المعلومات الموجودة أو يفأجئ بالكم الهائل من المعلومات التى لا يعرفها وهنا تبدأ مراحل الاحباط تدخل إلى قلبها وتبدأ هذه الجبال بالتصدع, لذلك تروى أخي العزيز في العلم فهو شيئ لايمكن الحصول عليه بالرغبة والهمة بل يحتاج إلى الوقت وإلى التخطيط العلمي الصحيح .

تجربتي تتلخص في النقاط الأربعة التى تحدثت عنها في كلا المقالان, أضف إليهم التدوين وحب مساعدة الناس فهو أحد الأمور التى تمدني بالهمة, وهذه النقاط كانت الثقة بالله وبعدله, وإدراك أهمية العلم وتحرير العقل من مفهوم الدراسة بحسب متطلبات العلم وآخيرا عدم الأستعجال وهي نقطة تحتاج أن تتذكرها بشكل دائم فأنا وقعت فيها كثيرا عندما كنت أمر بمرحلة الضياع وعدم تحديد الطريق الصحيح, الهمة أول محركاتها برائي المتواضع الثقة بالله وبعدها تأتي أهمية العلم بالنسبة لك فإما تقرر أن تكون دراستك للعمل وإيجاد الوظيفة وحينها هذا المقال لن يفيدك بشيئ وإما أن تكون متحدي في الطراز الرفيع وتقول في نفسك إحذروا يامهندسي الكمبيوتر فلقد دخل متحدي كبير على الساحة ويريد أن يأخذ أماكنكم واحدا تلو الآخر فهل من متحدي ؟ , أنا هكذا بدأت وعلى هذا الأساس عملت همة جعلتني عندما ألقي رأسي على مخدة الفراش متعبا من القراءة والدراسة والكتابة أقول في نفسي متى سوف يحين الصباح لكي إبدا الدراسة والقراءة همة دفعتني لأن أبدا الدراسة وأنا أملك أسوء لغة أنكليزية موجودة بينكم. من أين حصلت عليها ؟ حصلت عليها من زرع الثقة فيني يوما بعد يوم بأن مميز وبأني قادر على الوصول لكن ليس بشهر أو اثنان بل بسنة وسنتان وبتخطيط دقيق وقراءة يومية للكتب العلمية وليس المقالات والمنتديات والمدونات, أسس نفسك بشكل صحيح وأعطي لنفسك الوقت الكافي ولاتفكر بأن لو أنهيت الشهادة هذه وتلك وقرأت هذا الكتاب وذاك سوف أنجح, لا ابدا, يجب أن تصل كل يوم إلى نتيجة تقول أن كلما تعلمت أكثر إزداد جهلي أكثر فعندما تتعلم عن الأيبي ترى أن هناك باكيت وعندما تتعلم ماهي الباكيت تجد الطبقات وكلما دخلت أكثر وجدت أمامك أبواب أكثر وأسئلة أكثر, هذه هي لذة العلم وهذا ما قصدته في نقطة الوصول إلى أهمية العلم وهو ما لم نعيه ونحن صغار ونضيعه ونحن كبار إبحث عنه وحرر عقلك من مفهوم العلم التجاري فهو بلا دافع وبلا مستقبل حقيقي وتذكر أن كل الهمم والمعنويات اللازمة فيك أنت وحدك فلو في حال لم تجد من يساعدك على رفعها فأبحث عنها في داخلك وسوف تجدها وعن تجربة ودمتم بود.

أيمن النعيمي - سوريا

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس و رئيس التحرير

م.أيمن النعيمي

المحـررون

م.نادر المنسي	م. سامي أحمد الرجعي	م. أنس المبروكي
م.خالد عوض	م.أحمد زهران	---
م.أنس المبروكي	م. أحمد هيكل	---
م. شريف مجدي	م.فادي الطه	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل

www.networkset.net

NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية

Magazine NetworkSet

أول مجلة عربية متخصصة
في مجال الشبكات

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

أول مشروع عربي لترجمة
المواد العلمية و التقنية

YouTube

قناة المدونة على يو تيوب

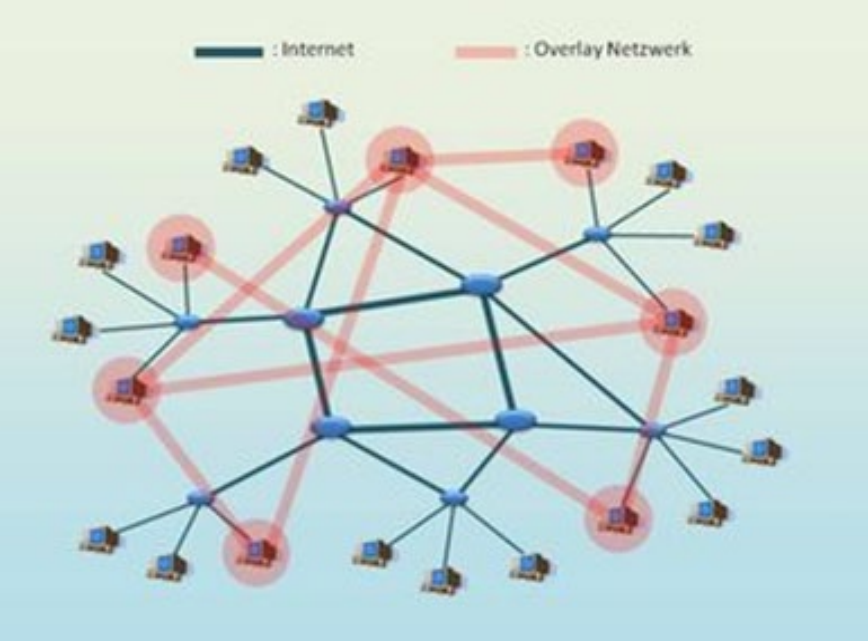
قسم خاص بالأسئلة والاجوبة

الشبكات الافتراضية أنواعها وتطبيقاتها

بعض البرامج الموجودة على أجهزتنا مثل برنامج الـ Skype وبرنامج الـ Torrent وغيرها، وكل يوم يظهر برنامج يحتاج إلى عمل شبكة خاصة بمستخدمي هذا البرنامج وشبكة خاصة بذلك البرنامج ولكل واحدة طبيعتها المختلفة عن الأخرى وهذا يعني الحاجة إلى وجود العديد من الشبكات على الانترنت. وبالطبع ليس من المنطق أن نقوم بتغيير بروتوكولات الانترنت لتتلاءم مع كل شبكة أو برنامج وهذا ما جعل المهتمين يركزون جهدهم على الشبكات الافتراضية.

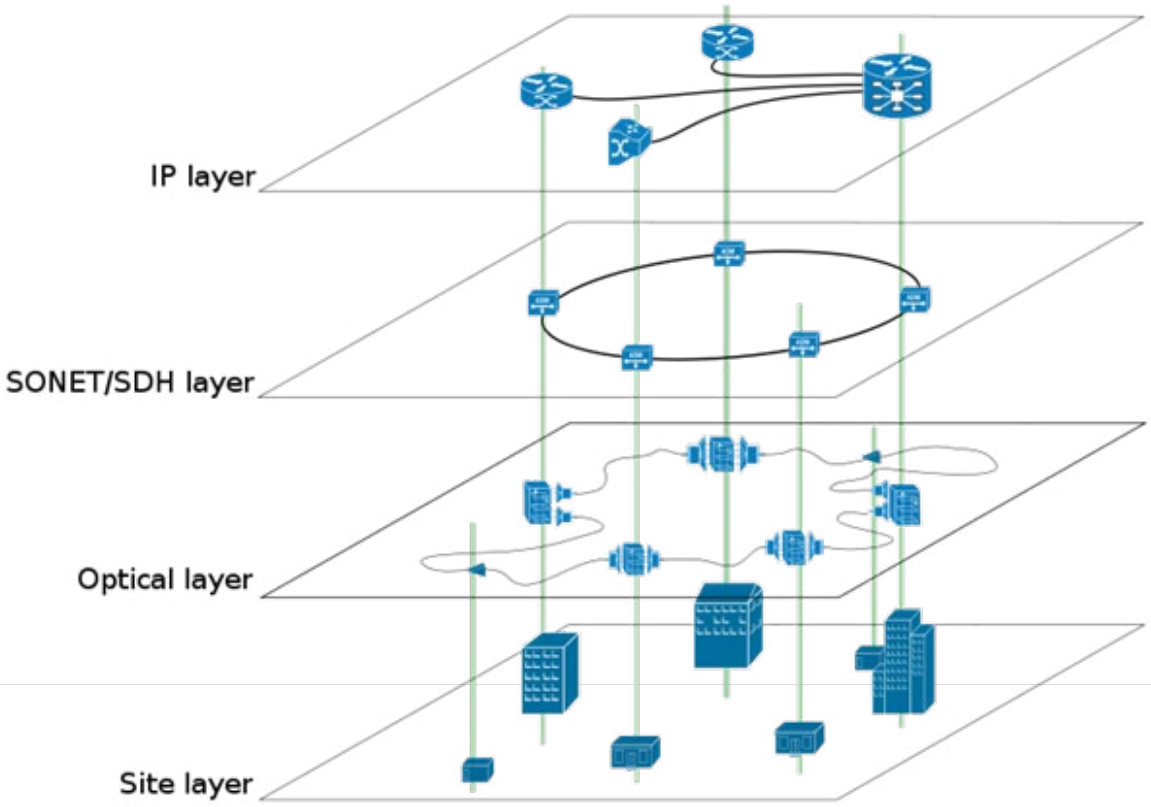
فأكثرنا استعمل الشبكات الافتراضية (اقصد بشكل عام وليس الـ VPN بالتحديد)، ولكن البعض لا يعرف بطبيعتها ولا كيفية عملها و حتى لا يعلم أنها شبكات افتراضية، لهذا في هذا المقال سنتعرف عليها وطريقة عملها ونتناول تطبيقات خاصة منها.

فالشبكات الافتراضية هي شبكات يتم إنشائها فوق شبكة موجودة مسبقا مثل الانترنت. وكل شبكة تخصص لبرنامج معين، فمثلا شبكة تدعم برامج multimedia streaming كما في برنامج BBC iPlayer وشبكة خاصة ببرامج الألعاب الاونلاين Multiplayer Online Games مثل برنامج Hamachi و Tunngle وتوجد برامج أخرى لإغراض مختلفة مثل برامج Cloud Computing وغيرها. وجميع هذه الشبكات يتم إنشاءها من دون تغيير على شبكة الانترنت وكل واحدة لها طرق عنونة مختلفة بعناوين تسمى Logical IPs وبروتوكولاتها وطرق الـrouting الخاصة بها تختلف من شبكة إلى أخرى.

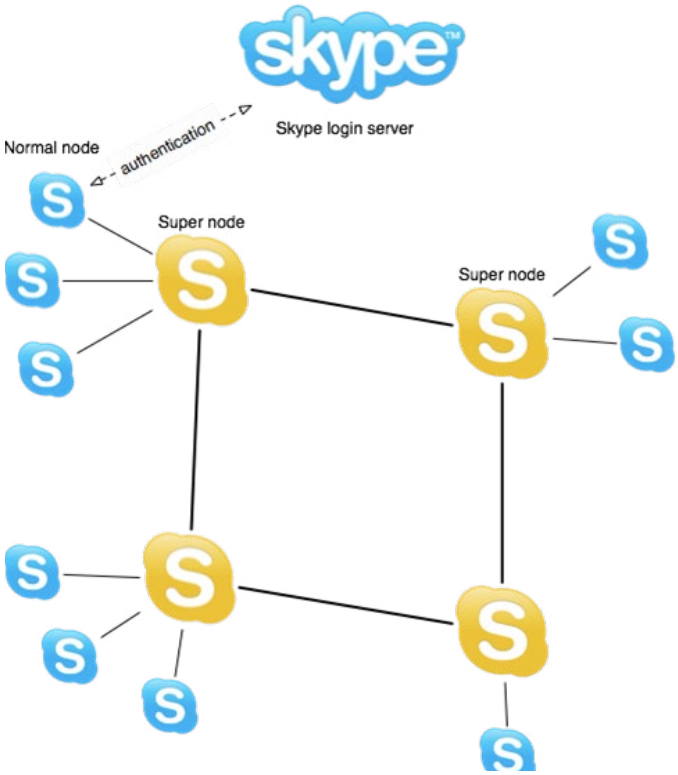


من الفوائد الأخرى للشبكات الوهمية أنها تساعد على بناء شبكات لغرض التجارب والأبحاث مثلا وتكييفها حسب الرغبة أو حسب البرنامج المستخدم إضافة إلى إمكانية توسيعها أو تغييرها حسب الحاجة.

من العيوب التي تنقص مثل هذه الشبكات هو إن الوصول للجهاز المطلوب يكون غير مباشر وهذا يؤدي إلى التقليل من أداءها إلى جانب كونها أكثر تعقيدا مقارنة بالشبكات التقليدية. ولكنها تتشابه معها في أنها تتكون من طبقات غير انها تختلف عن طبقات الـ OSI Model المعروفة، وهي من الأعلى IP Layer و SONET/SDH Layer و Optical Layer و Site Layer. وكما مر سابقا فان عملية الـRouting تترك لمصمم الشبكة، لذلك توجد عدة خوارزميات لهذا الغرض وحسب البرنامج الذي يتم تطويره فمثلا هناك طريقة للـ Routing تسمى بـ Key-Based Routing وتعني بشكل مختصر إن الجهاز في الشبكة إما لديه العنوان أو key المطلوب أو لديه لنك إلى جهاز قريب من الجهاز الذي لديه العنوان المطلوب وتتم العملية هذه عبر جدول يسمى Distributed Hash Table. أما الـ topology المستخدمة فتختلف حسب المصمم ولكن بشكل عام تعتبر الـ Ring هي أكثر topology شائعة الاستخدام.



أخيرا سوف نتعرف عن قرب على أكثر الشبكات الوهمية نجاحا وهي الـ Skype وكيف تستغل هذه الشركة أجهزتنا وتليها نظرة سريعة على شبكات مشاركة الملفات Torrent.



يعتبر الـ Skype من برامج Peer to Peer ويقدم خدمات الـ VOIP إضافة إلى دعمه لخدمات الشات instant messaging ومكالمات الفيديو video conference. تم تطوير هذا البرنامج في عام 2003 و يتجاوز عدد مستخدميه 663 مليون مستخدم حسب إحصائيات 2010 ويتوقع أن يصل إلى 1 مليار بحلول عام 2015. وبهذا تعتبر الـ Skype من اكبر الشبكات الوهمية في العالم وهذا يبين مدى التعقيد في بناء هذه الشبكة.

عند استخدام هذا البرنامج لا يحتاج المستخدم إلى IP الجهاز الآخر لبدء الاتصال حيث تتم العملية أوتوماتيكيا كما سنتعرف عليها بعد قليل. أما المعمارية التي تم إنشاء شبكة Skype وفقها فهي غير معلنة للعامة ولكن أصبحت مفتوحة للجميع بعد أن قام عدد من الباحثين بدراستها وتحليل الترافيك والاتصالات. حيث تتكون من نوعين من الأجهزة الخاصة بالمستخدمين أو بمصطلح الشبكات nodes، وهي المستخدم العادي أو الـ node normal والنوع الآخر يسمى super node وهو نفس الـ node العادي ولكن يتميز بإمكانيات معينة يتم اختيار هذه الـ nodes وفقها مثل سرعة الاتصال لهذا الـ node مع الانترنت وإمكانية الوصول المباشر لهذا الـ node أو بمعنى آخر يجب أن لا يستعمل الـ NAT في عنونته ويكون الـIP الخاص به هو نفسه global IP إضافة إلى طول المدة الذي يتواجد فيه هذا الـ node وبالطبع كلما يزداد وقت استعمال الـ skype بشكل متواصل يزداد احتمالية اختيار هذا المستخدم كـ Super node.

عند فتح برنامج الـ skype والبدء بالاتصال بالسيرفر يقوم السيرفر بتدقيق الـ username والـ password ومن ثم يحدد نوع الـ node، فإذا كانت node عادي يرسل قائمة تحتوي على عناوين حوالي سبعة من الأجهزة الـ super تخزن في cache الجهاز العادي ويزداد هذا العدد بمرور الوقت وقد يصل إلى المئات. أهم فائدة من هذا الـ super (وهنا تتم عملية استغلال أجهزة المستخدمين) هي عند عمل مكالمة بين طرفين يقوم المستخدم الأول بالاتصال بأحد الـ super والتي تحتوي بدورها على عناوين مجموعة من المستخدمين العاديين، يبحث الـsuper بقائمة العناوين التي لديه فإذا لم يجد عنده عنوان المستخدم الآخر يتعاون مع باقي الـ super nodes في إيجاده، وبشكل عام كل ثمانية super nodes تتعاون فيما بينها لإيجاد عنوان معين.

البرنامج الآخر الذي يعتبر كمثال لشبكة تستعمل مبدأ الشبكات الافتراضية هو الـ BitTorrent. يعتبر BitTorrent من أشهر برامج مشاركة الملفات Peer to Peer وهو مصمم بشكل عام لتحميل الملفات الكبيرة الحجم وخصوصا ملفات الفيديو التي يجري تشغيلها لاحقا وليس العرض المباشر Real Time Streaming.

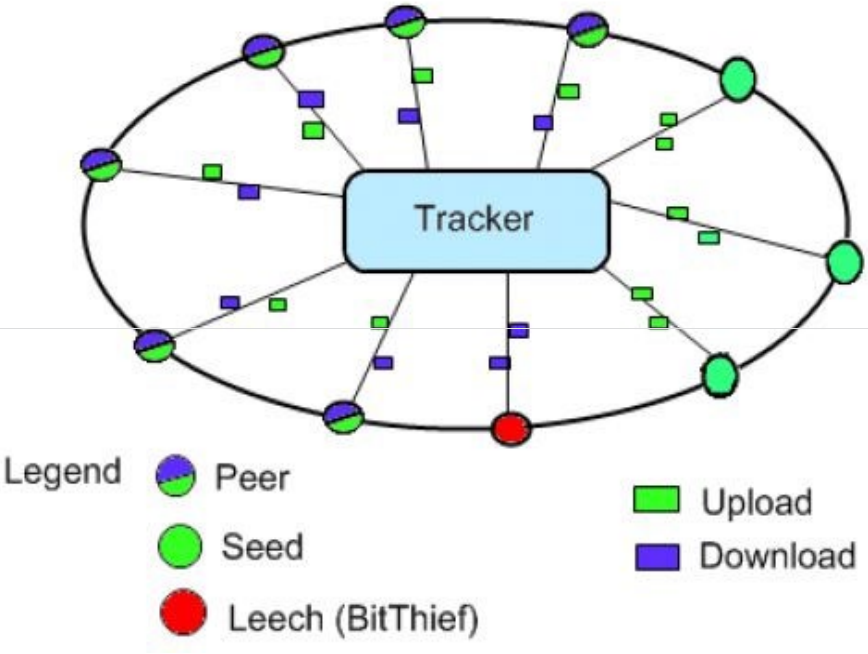
يعتمد الـ BitTorrent بالأساس على تقسيم الملفات إلى أجزاء ذات حجم ثابت تسمى chunks، وتنتشر هذه الأجزاء أو الـ chunks على عدة أجهزة ويستطيع المستخدم تحميل الملف على شكل chunks من عدة أجهزة وبشكل متوازي Parallel مما يقلل الحمل أو Load على سيرفر واحد ولا ننسى إن الـ BitTorrent يستعمل أجهزة المستخدمين العادية كسيرفرات لباقي الأجهزة الأخرى وهذا يجعل سرعة الاستجابة محددة بإمكانيات هذه الأجهزة ويظهر واضحا عند تحميل فايل تكثر عليه الطلبات، وعلى الرغم من هذا إلا انه يعتبر أفضل من السيرفر الواحد عند استعمال الـ HTTP مثلا.

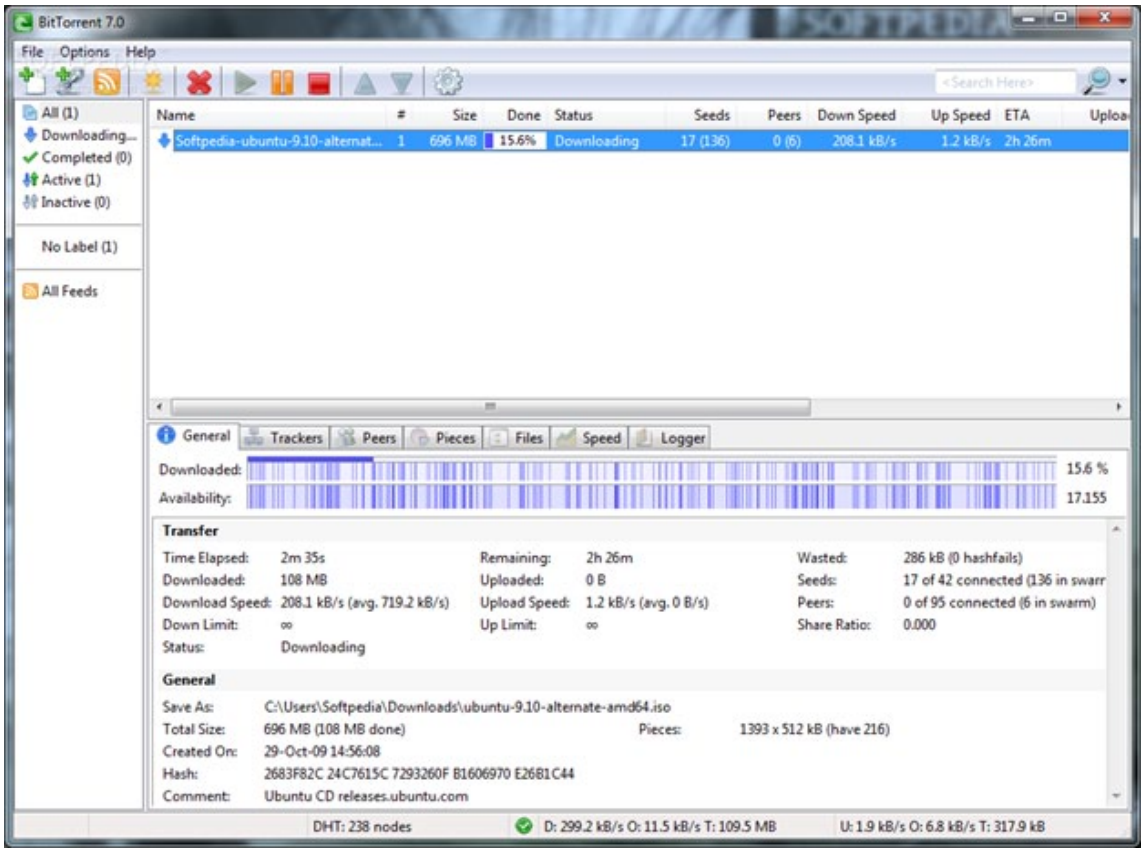
لنتعمق قليلا في طريقة عمل الـ BitTorrent، فعندما يضاف فايل إلى الـ BitTorrent يقوم بعمل فايل بامتداد (torrent.) يحتوي على معلومات تسمى metadata وهي:

- اسم وطول الملف.
- عنوان الـ tracker وهو عبارة عن URL السيرفر المركزي الذي يقوم بإدارة التحميلات.
- الـ checksum لكل chunk ويتم توليده باستخدام خوارزمية تسمى SHA-1 hashing algorithm حيث يفحص كل chunk بعد اكتمال تحميله.

وكما مر قبل قليل فان الـ BitTorrent يجمع بين Peer to Peer في عملية النقل وبين Client-Server في عملية إدارة التحميلات عن طريق الـ tracker.
ولكي نفهم كيفية عمل الـBitTorrent سنتعرف على دورة حياة فايل معين يتم تحميله عبر الـBitTorrent:
أولا وقبل كل شي لنتعرف على بعض المصطلحات، فكل مستخدم أو جهاز لديه جميع أجزاء الفايل أو الفايل بكامله يسمى seeder، والجهاز صاحب أول نسخة من الفايل يقوم بتوزيعه على الباقين. أما المستخدم الذي سوف يقوم بالتحميل فيسمى leecher وقد يكون لديه أجزاء من الفايل. وبعد أن يكمل تحميل جميع أجزاء الفايل يتحول إلى seeder ليخدم باقي leechers وهكذا.
لذلك فالـ tracker لديه معلومات عن جميع seeders و leechers وهذه الثلاثة مجتمعة تسمى torrent.

الآن نفرض أن مستخدم يريد تحميل فايل معين، بداية يقوم بالاتصال بالـ tracker حيث يقوم الأخير بتزويد المستخدم بالأجهزة التي لديها هذا الملف. إلى هنا ينتهي عمل الـ tracker ويتحول الاتصال من client-server إلى peer to peer، ومن ثم تبدأ عملية النقل من المستخدمين الآخرين ولا يشترط تحميل أجزاء الملف بشكل متسلسل.





ختاما بعد تناولنا لهذه البرامج أتوقع تغيرت نظرتكم لها وخصوصا إن الكثير منا يريد معرفة طريقة عمل البرامج التي يستخدمها و إن شاء الله يكون عندي الوقت الكافي (لانشغالي بالدراسة والامتحانات) في الأعداد القادمة من المجلة لأشرح الكيفية التي تعمل عليها برامج أخرى تستعمل الشبكات الافتراضية في عملها.

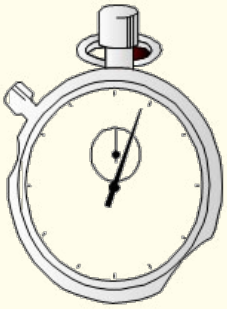
Cron: automation of the commands

فى خلال قراتى للمجله فى العدد السابق قراءت مقال المهندس انس المبروكى عن كيفيه تعديل الاوامر على رواتر سيسكو حتى تعمل فى وقت محدد على الروتر بامر يدعى kron وهو موجوده مثله فى UNIX فقلت لماذا لا اكتب عنه هو الاخر ولكن من وجه نظر اليونكس وليس من وجهه نظر الشبكات .

فى البدايه فى AIX Unix لا يوجد فقط امر واحد لكى تتمكن من جعل الامر يعمل على النظام فى وقت محدد ولكنهم ثلاثه اوامر كالتالى :

at , batch , and cron

At command - 1



وهو يمكنك من تحديد وقت محدد لتشغيل امر معين ولكن هذا الامر يعمل مره واحده فى الوقت المحدد له ثم بعد ذلك ينتهى ولا يعمل مره اخرى اى انه لا يكرر نفسه not repeated

ويكون طريقه كتابته كالتالى :

At <time you want to run command in>
Type the command that you want
<ctrl+d>

ومثال على ذلك كالاتى :

Ctrl-d تعنى انك انتهيت من كتابه الامر او الاوامر التى تريد تنفيذها فى الوقت المحدد

```
# at now +2 mins
banner hello > /dev/tty3
<ctrl-d>
```

Batch command - 2

امر batch يعمل مثل at تماما فانت تقوم بتحديد الامر او مجموعه الاوامر التى تريد منها ان تعمل فى وقت محدد ولكن لا تحدد مثل هذا الوقت لانه الذى سيقوم باختياره هو النظام نفسه .

لتوضيح ذلك فى حاله at command فانت تقوم بتحديد الاوامر التى تريد تنفيذها والوقت الذى تريد من النظام ان يقوم بتنفيذها فيه اى كانت حالته بمعنى اذا كان مشغول ويعالج عمليات اخرى او لا فهذا لا يعينك المهم انه فى هذا الوقت يقوم النظام بتشغيل هذه الاوامر اما فى حاله batch command فان النظام يقوم بتشغيل هذه الاوامر عندما يكون الحمل load الموجود على المعالج قليل وهنا يكمن الفرق بين ال at and batch commands .

فكما هو واضح انك لا تحدد وقت معين بعد كتابه الامر ولكنك تتركه للنظام لكى يقوم بتحديده

```
# batch
banner hello > /dev/tty3
<ctrl-d>
```

Cron command - 3

وهو اهمهم على الاطلاق حيث انه repeated فانه يقوم بتكرير نفسه اى انك ممكن ان تقوم بجعل امر معين يعمل كل يوم على النظام فى ساعه ودقيقه معينه . فهذه احد المهمام التى تستطيع ان تقوم بها من خلال cron command ونحن نستخدمه كثيرا فى الحياه العمليه خاصه فى موضوع backup او اخذ نسخ احتياطيه من النظام او من البيانات الموجوده عليه لانه فى الغالب ناخذ النسخه الاحتياطيه من البيانات فى الاوقات التى لا يعمل فيها احد على النظام لذلك ال cron مهم جدا معرفته لتشغيل النظام .

ولكتابه ال entry الخاص بال cron فعليك اتباع طريقه معينه حتى تكون ادخلت ال entry بشكل صحيح الى الملف الذى ستحفظ فيه هذه البيانات .

Format:

```
minute hour date month day-of-week command
```

Minute : الدقيقه التى ستعمل فيها والقيم المتاحه لها (0:59)

Hour : الساعه التى سيعمل فيها والقيم المتاحه (0:23)

Date: فى اى الايام فى الشهر ستقوم بعمل تشغيل لها والقيم المتاحه (1:31)

Month : فى اى الشهور ستقوم بتشغيلها والقيم المتاحه لها (1:12)

Day-of-week: فى اى ايام الاسبوع ستقوم بتشغيلها والقيم المتاحه لها (0:6)

وهنا 0 تعنى الاحد , 1 تعنى الاثنين وهكذا حتى تصل الى 6 والتى تعنى يوم السبت وهذا نظرا لانه فى هذا الامر يعتبر يوم الاحد هو بدايه الاسبوع.

لكى نفهم هذا الامر دعنا نضرب امثله على :

1 - انفترض مثلا انك تريد تشغيل الساب كل يوم الساعه السابعه صباحا .

Entry : * 6 * * * startsap

وهنا * تعنى كل القيم فمثلا المثال السابق نستطيع قرائته كالتالى فى اى دقيقه فى اى يوم فى اى شهر عند الساعه السابعه قم بتشغيل الساب .

2 - مثال اخر : نريد ان نشغل الاوراكل من كل يوم احد الى الجمعه الساعه الثامنه والربع كل يوم

Entry : 14 7 * * 0 - 5 startoracle

اى انك تستطيع قرائته كالتالى فى اى يوم فى اى شهر فى السنه يوافق من الاحد الى الجمعه عليك ان تقوم بتشغيل الاوراكل الساعه الثامنه والربع صباحا .

```
# crontab -l
#
#COMPONENT_NAME: (CMDCNTL) commands needed for
#basic system needs
#
#0 3 * * * /usr/sbin/skulker
#45 2 * * 0 /usr/lib/spell/compress
#45 23 * * * ulimit 5000;
/usr/lib/smdemon.cleanu > /dev/null
0 11 * * * /usr/bin/errclear -d S,O 30
0 12 * * * /usr/bin/errclear -d H 90
```

فى الشكل الموضح قائمه ال entries التى يقوم النظام يتنفذيها والتى يمكن استعراضها باستخدام الامر التالى crontab –l .

أهم خمس شهادات تقنية بحسب دراسة NetworkSet

بعد فتح ساحة النقاش على أفضل خمس شهادات في قطاع الـ IT في مدونة NetworkSet والتى شارك فيها 15 شخص (قليل جدا) وجدت بعض الملاحظات على النقاش وأستخلصت النتائج منها وأعرضها عليكم كأسلوب جديد في طرح المقالات على المدونة .

قبل أن أخوض في النتائج يتوجب علي أن أوضح أهمية هذا النوع من النقاشات, فالفكرة التى أحاول الوصول إليها من النقاش هو أستخلاص الدراسات والنتائج المبنية على العقول والتجارب العربية لأناس تعرفوا على الواقع العملي وخصوصا أن المواقع الأجنبية تغص بمثل هذا النوع من المقالات لكن لاتفيدنا ولاتقربنا لهدفنا الحقيقي ألا وهو السوق العربية لأن ساحات العمل تختلف أختلافا كليا بيننا لذلك أتمنى من الجميع أن يساهم في إثراء مثل هذه النقاشات لأن فوائدها مستقبلا ستكون كبيرة جدا على سوق الدراسات والأبحاث العلمية العربية, كما يمكنك طرح أي نقاش ترغب به مع ضرورة توضيح وجهة نظرك فيه ويفضل أن يكون النقاش عن أفضل خمسة أو أهم عشرة أشياء وبكلام آخر فلكن النقاش مبني على الأرقام حتى تكون هناك نتائج ودراسات نستخلصها من النقاش وأنا بدوري سوف أخذ أفكار هذا النقاش وأعيد صياغتها بنفسي على شكل مقال أقدم فيه زبدة الكلام زائد خبرتي البسيطة في ما تم تداوله.

نعود الآن إلى نقاشنا الأساسي, في البداية أنا طرحت النقاش ولم أحدد فيه عالم الشبكات بل فضلت أن يكون النقاش عاما وتدخل فيه كل مجالات التقنية لكن النتائج أغلبها صب في صالح الشبكات كون أغلبية الزوار مهتمين بهذا التخصص بشكل مباشر.

1 الشهادة الأولى MCITP

حصلت هذه الشهادة Microsoft Certified IT Professional على المرتبة الاولى وبلا منازع وبأغلبية كل الاشخاص الذين أبدوا أرائهم معنا, الشهادة ومن الخبرة التى شاهدتها في الساحة العملية مطلوبة في كل مكان فلا يوجد مكان لايوجد فيه نظام مايكروسوفت ولا توجد شركات لاتملك دومين سيرفر أو أي خدمة من خدمات سيسكو لذلك فالأولوية الكبرى في عالم الشهادات في السوق العربية هو لشهادات مايكروسوفت وتحديدا MCITP بالنسبة لشهادة الـ MCSE هي تقريبا في نفس المستوى ولايوجد أختلاف جوهري بينهما غير أن الأولى هي لسيرفر 2003 والثانية لسيرفر 2008 لكن بسبب تحول الكثير من الشركات إلى الأصدار الجديد حلت هذه الشهادة مكان الأولى وأصبح الطلب عليها أكبر لكن من وجهة نظري لو كان الشخص الذي يعرض الوظيفة ويطلب MCITP خبير في مجال التقنية فهو سيعي هذه الحقيقة ولن يمانع من توظيف شخص يملك MCSE أما لو كان جاهلا فسوف يقف الأمر عائقا بينك وبين الوظيفة , لهذه الشهادة نوعان إما MCITP - SERVER ADMINISTRATOR أو MCITP - ENTERPRISE ADMINISTRATOR والصورة سوف توضح الأختلافات .

2 الشهادة الثانية CCNP

الشهادة الثانية في الترتيب نالتها سيسكو الشركة العملاقة في مجال الشبكات والتى مازالت تسيطر على أكبر سوق في العالم العربي في مجال المعدات الشبكية وتحديدا في شهادة Cisco Certified Networking Professional (Routing & Switching) الحقيقة الحديث عن هذه الشهادة وعن مدى أهميتها قد يفأجئك بعض الشيئ وقبل أن أتحدث عنها أعود وأذكر أن ما أتحدث عنه هو أراء شخصية في المقام الأول قد تصيب وقد تخيب, أهمية الشهادة في سوق العمل كبيرة ومطلوبة بكثرة لكن على الساحة العملية وفي قلب الوظائف قد تفأجئ بأن ماتعلمته وتعبت عليه لن تستخدم ربعه في العمل فهي أسم ومنصب أكثر مما هو فائدة حقيقية للسوق والذي يقوي مكانتها فوق مكانة CCNA هو كلمة محترف عوضا عن مبتدأ والتى تشكل فارق كبير بالنسبة لأصحاب العمل وخصوصا أن الحصول عليها لم يعد يشكل صعوبة كبيرة, الشهادة بشكل عام ولوناقضت نفسي قليلا قوية بالفعل وأفضل مافيها هو الأمتحان الجديد الخاص بحل المشاكل لكن تبقى الأستفادة على الساحة العملية الحقيقة منها شيئ غير منطقي لأن السوق العربية ومدى ضخامة الشركات مازال محدود بعض الشيئ .

3 الشهادة الثالثة CCNA

تعود سيسكو لتفرض نفسها مرة ثالثة بين المشاركين في الحوار وتحصل على المرتبة الثالثة لكن هذه المرة مع شهادة المبتدأ Cisco Certified Network Associate (Routing & Switching) وما لاحظته من خلال الأراء أن الجميع يذكر كلتا الشهاداتان في نفس الوقت وهذا التعارض في الأراء يعود إلى كون المشارك وصل معي إلى نفس النتيجة السابقة وهي المتطلبات الحقيقة لسوق العمل ومدى الاختلاف بين المسميات لذلك نجد المشاركات تضم كلتا الشهاداتان, الشهادة قوية ومفيدة جدا ولو تعلمتها بشكل صحيح وبتركيز كبير سوف تحصل على نتائج مستقبلية في طريقك للتميز في هذا العالم فأنا بدأت منها ووجدت إثارة كبيرة في دراستها, بغض النظر عن كونها شهادة تتبع لسيسكو إلا أنها تعتبر (رائي شخصي) أم الشهادات في عالم الشبكات فهي تركز على المعلومات العامة أكثر مما تركز على سيسكو نفسها لذلك لا تتجاهلها ابدا وأعطها متسع كبير من الوقت وبالنسبة لي شخص فاهم لهذه الشهادة بنسبة 90 ٪ أفضل من شخص حاصل على CCNP, وطبعا هذا لايعتبر إنقاصا بحق من يحمل هذه الشهادة فأنا أحملها أيضا لكن لو تحدثنا عن الساحة العملية العامة وضع تحتها خطان وثلاثة خطوط فهي بلا فائدة إلا لو كانت الشركة تعمل في مجال الأنترنت أو لديها أجهزة كثيرة جدا في شبكتها .`

4 الشهادة الرابعة VMWARE

حصلت VMWARE على المركز الرابع في ترتيب الشهادات بحسب أراء المشاركين وأود قبل الخوض في تفاصيل شهادات هذه الشركة أن أقدم ملاحظة صغيرة عن سبب تصويتي لصالح هذه الشهادة فأنا لم أصوت لها عن خبرة مع الواقع العملي لأن لم أصادف شركة لديها تعامل كبير مع سوق الاجهزة الوهمية لكن وضعتها كتصور مستقبلي لمجال أعتقد أن المستقبل كبير بالنسبة لها وخصوصا أنها توفر مميزات كثيرة للشركات وإن كنت أختلف مع نصف الكرة الأرضية في فكرة التوفير التى تمنحنا أياها هذه التقنية لأن أضع عليها الكثير من النقاط والتساؤلات الى ت كانت نتيجة بحث طويل ومعمق عنها ولا اريد الخوض فيها في الوقت الحالي, لـ VMWare نوعان من الشهادات , الأولى تتحدث عن الـ Desktop Virtualization وهي في مستويان مبتدأ VCA ومحترف VCP والثانية Datacenter Virtualization وهي في ثلاث مستويات مبتدأ VCA محترف VCP متخصص VCDX , ولو سمح لي الوقت مستقبلا فقد أخصص مقال كامل عنها

5 الشهادة الخامسة LPIC

على مبدأ أن لسوق أنظمة التشغيل النصيب الأكبر في عالم الـ IT بشكل عام قررا المشاركين أختيار أحد شهادات لينوكس الأحترافية وهي Linux Professional Institute Certification, لا أملك أي خبرة في سوق لينوكس ولم أصدافه كثيرا في حياتي لكن بأعتقادي أن الشهادة مهمة ومفيدة جدا لمن يبحث عن أحتراف عالم الـ Network Software فهي تعتبر نقلة نوعية في مفهومك لأحتراف عالم لينوكس بحيث تخرجك من عالم CompTIA المتمثلة بشهادة Linux+ البسيط وتدخلك في عالم آحترافي يسمح لك أن تتطور وفق نظام مناسب وبتسلسل أحترافي يبدأ معك بمستوى المبتدأ ثم الأحترافي إلى الخبير وأنصح بها بشكل كبير أكثر من RHCE لأن الآخيرة تحتاج إلى جهد ووقت كبير ولاتملك تسلسل في الشهادات وحتى أكون منصفا لها الـ RHCE شهادة لها مكانة محترمة في العالم أجمع.

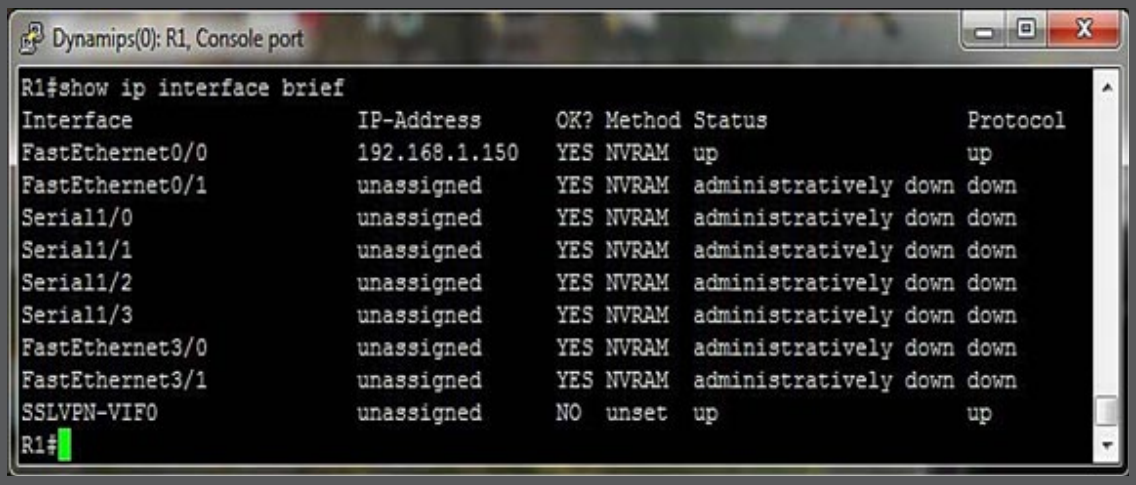
إلى هنا أكون قد أنتهيت من إعداد الدراسة التى هي أولى دراسة عملية نقوم بها على المدونة على أمل أن تتطور الحوارات مستقبلا ونطرح أفكار أعمق ونقاشات تمس العالم العربي بشكل مباشر وطبعا المجال سوف يكون مفتوح للنقاش فيه على المدونة, فالدراسة في الآخير هي أراء وخبرات منها عام ومنها شخصي ورائيك في الدراسة أكيد سوف يهمنا حتى نطور أكثر من أفكارنا وأفكار كل من يرغب بالحصول على شهادات عالمية تعزز إمكانية حصوله على وظيفة مرموقة في المستقبل ولاتنسونا من دعواتكم ودمتم بود.

أوامر التحقق من عمل الشبكة

عند التعامل مع معدات شركة سيسكو، هناك عدد من الأوامر المختلفة التي يجب على المهندس أن يكون على دراية بها لمعرفة الوضع الحالي للجهاز. يعتمد اختيار أي أمر سنستخدم على نوع العملية التي يجري التحقق من عملها. هذا المقال يلقي نظرة على بعض الأوامرالبسيطة التي يمكن استخدامها في معدات سيسكو للتحقق من أن الشبكة توجد في الوضع الطبيعي ويناقش المعلومات التي يمكن الحصول عليها نتيجة استعمال هذه الأوامر، وفي الختام سأحاول وضع جدول يضم مرادفات لهذه الأوامر في نظام تشغيل شركة الهواوي المسمى VRP.

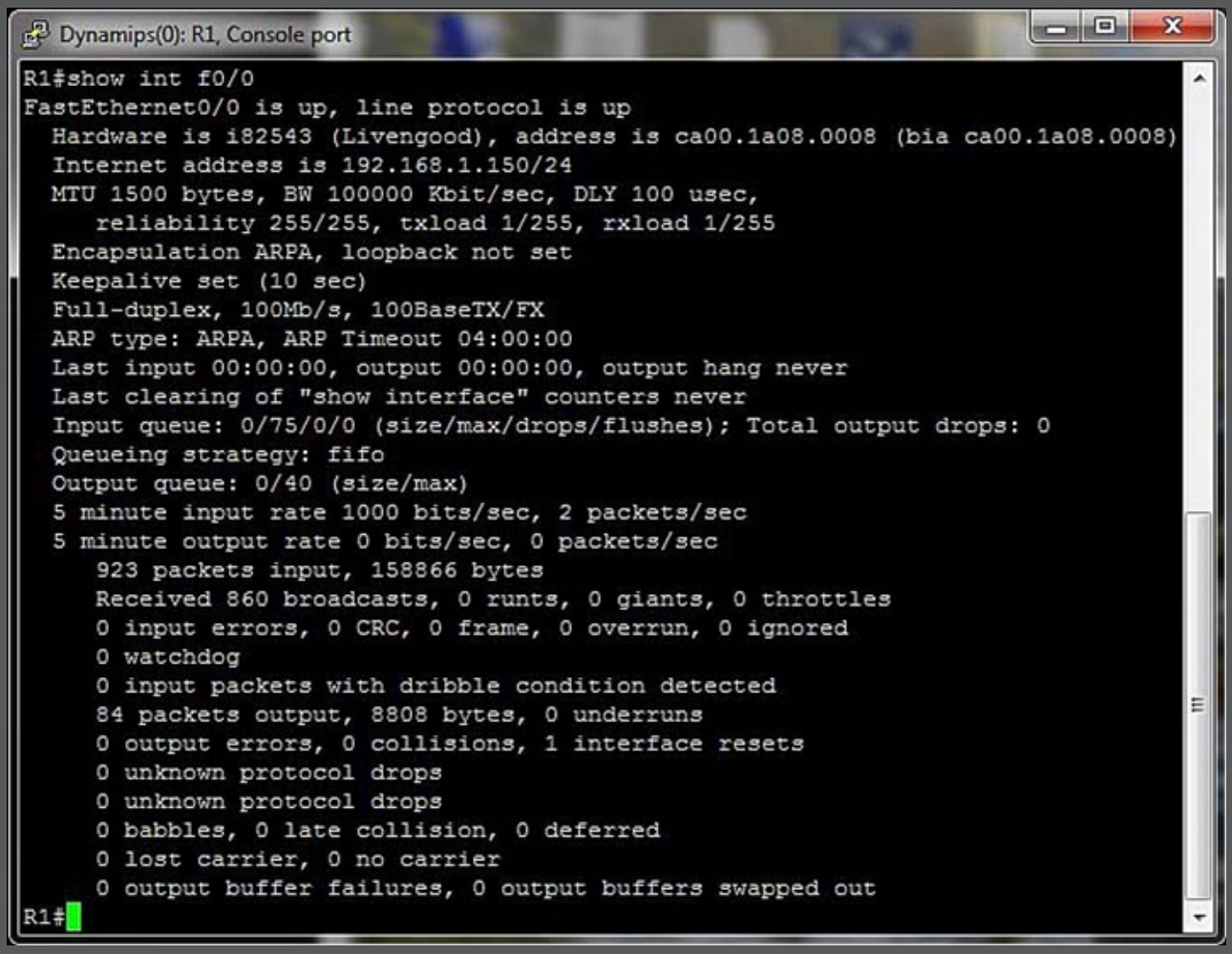
show ip interface brief :

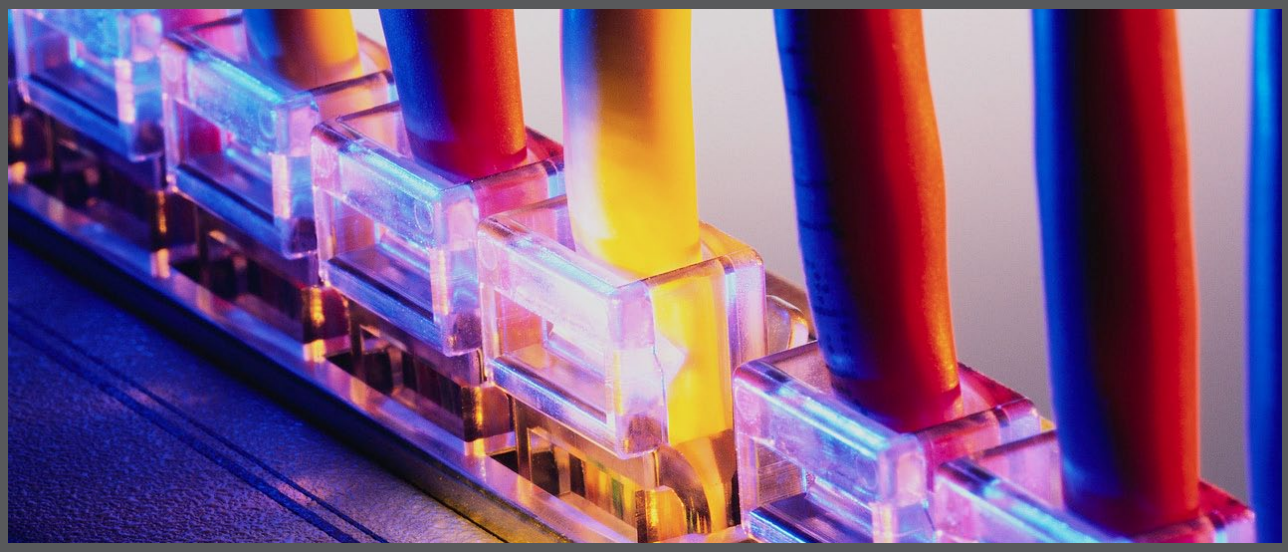
هذا الأمر عادة ما يستخدم من قبل العديد من المهندسين كخطوة أولى لاستكشاف الأخطاء وإصلاحها لذلك يحتاج منا مناقشته أولا. فهو يوفر لنا نظرة موجزة للوضع الراهن ل local IP interfaces و الحالة (status) الخاصة بها. المعلومات الهامة تتضمن إسم الواجهة ، عنوان IP address للواجهة، والحالة (physical) وحالة بروتوكول (data link). ويوضح الشكل أسفله أن هناك واجهة واحدة فقط معدة بعنوان (IP Address (192.168.1.150 ، وهي شغالة (0/Fastethernet0).



show interface :

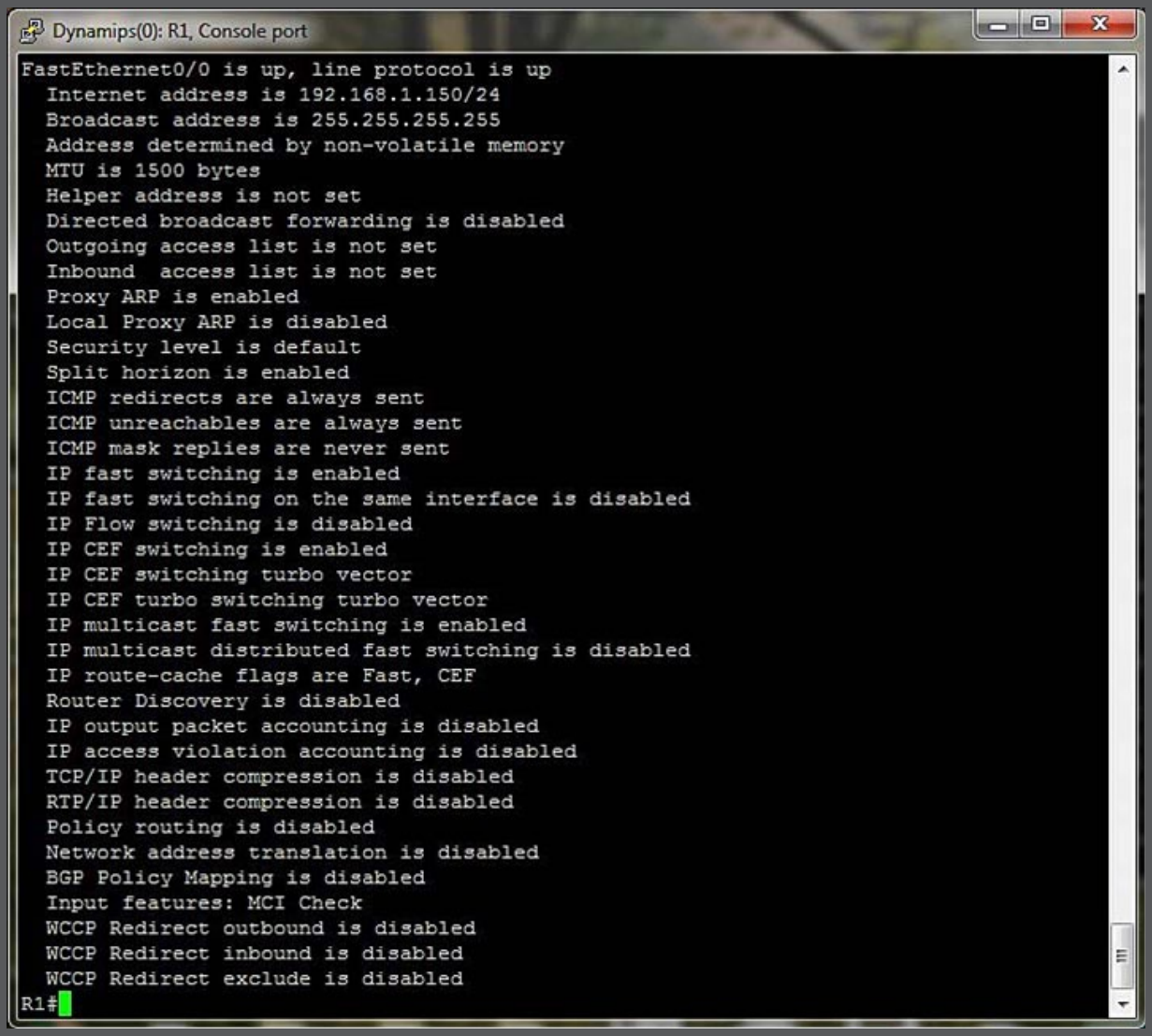
مثل أمر show ip interface brief ، فهذا الأمر يشمل الواجهة، حالة الواجهة (physical و data link معا) وIP address ، ويتضمن أيضا معلومات إضافية، بما في ذلك interface IP subnet mask ، إعدادات bandwidth ، إعدادات التأخير(delay)، إعدادات (queuing) ، بيانات ومعلومات بروتوكول(duplex data link و نوع ARP) ، وعدد من العدادات (counters) المختلفة التي يمكن استخدامها لمراقبة الواجهة. ويبين الشكل أدناه تطبيق أمر على واجهة0/fastethernet0 . وتبين النتيجة معلومات حول ، queuing (First In-First Out (FIFO) ، delay (100 usec) ، bandwidth (100 Mbps) ، subnet mask (/24) ، duplex (Full) وARP type (ARPA) .





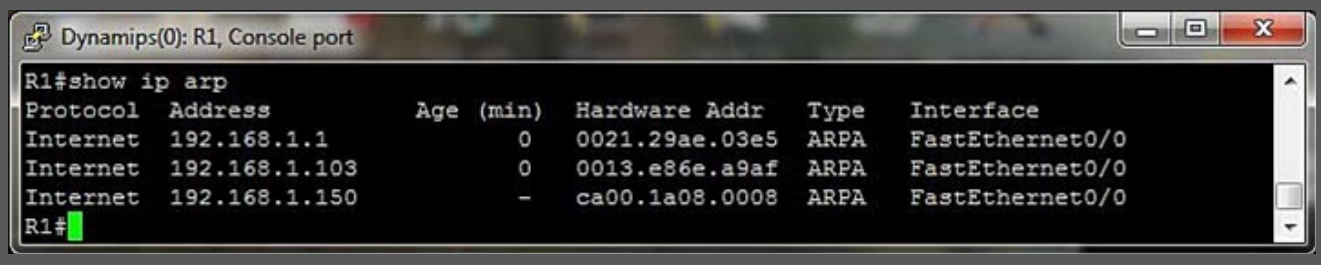
show ip interface :

هذا الأمر هو النسخة الكاملة لأمر ، ويتضمن كافة الإعدادات التي تخص IP protocol ، بما في ذلك عنوان IP و ACL ، mask ، نوع switching المستخدم و إعدادات compression ...



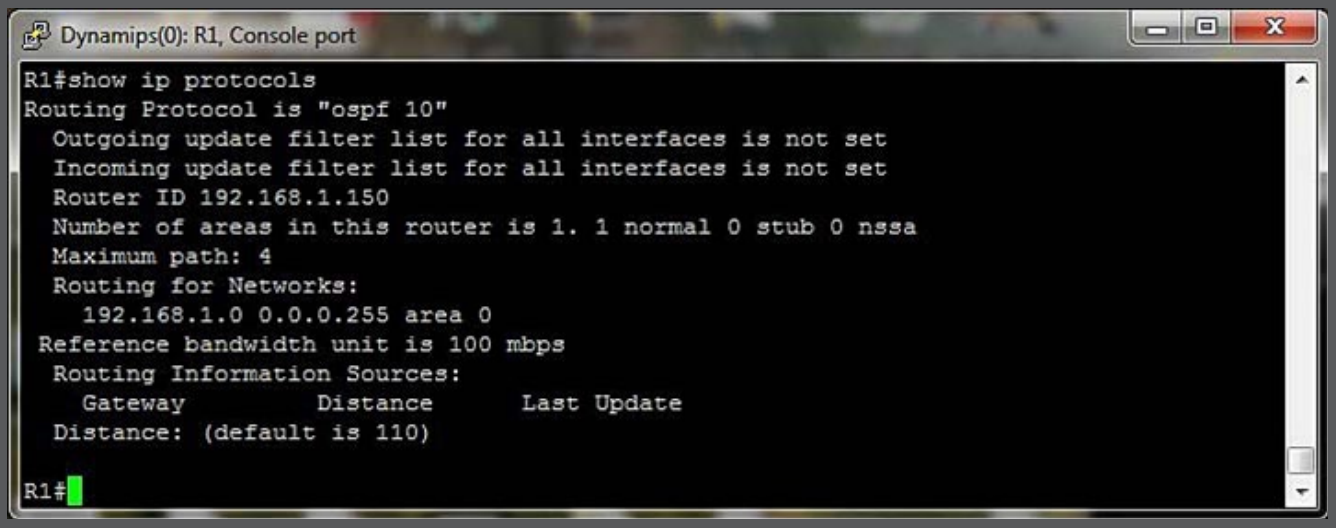
show ip arp :

يركز هذا الأمرعلى المعلومات تم الحصول عليها عن طريق بروتوكول ARP(Address Resolution Protocol)) الذي يستخدم لربط عناوين IP بعناوين MAC . سيقوم الجهاز بالبحث عن عنوان ARP الذي يلزمه لإرسال الترافيك إلى الجهاز المرسل إليه على الشبكة المحلية. ويبين الشكل 3 أجهزة مختلفة معروفة من قبل بروتوكول ARP ، بما في ذلك الجهاز المحلي (192.168.1.150) الكل على واجهة fastethernet0/0 .



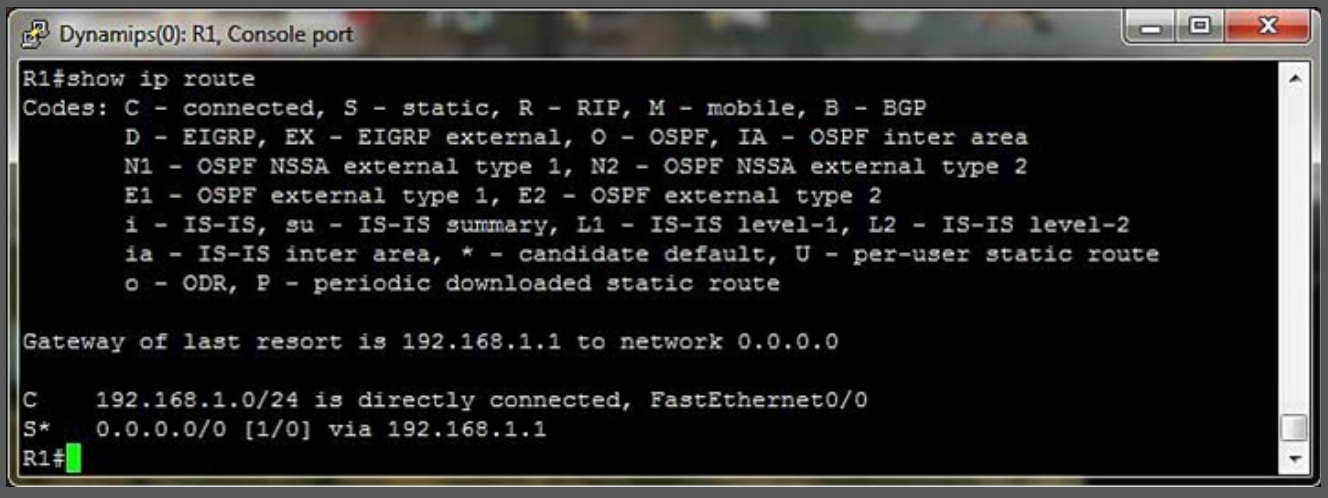
show ip protocols :

يتم استخدام هذا الأمر عندما يتم تشغيل أحد بروتوكولات التوجيه (routing) على الجهاز. وذلك للتحقق من أن بروتوكول التوجيه يشتغل كما هو متوقع. البيانات الدقيقة المستخرجة عن طريق هذا الأمر تعتمد على بروتوكول التوجيه الذي تم إعداده. الشكل أسفله هو لبرتوكول OSPF (Open Shortest Path First) ، وهو يظهر أن Router ID للجهاز المستخدم من قبلOSPF هو 192.168.1.150 وهو يوجه الترافيك للشبكة 24/192.168.1.0 باستخدام area 0 .



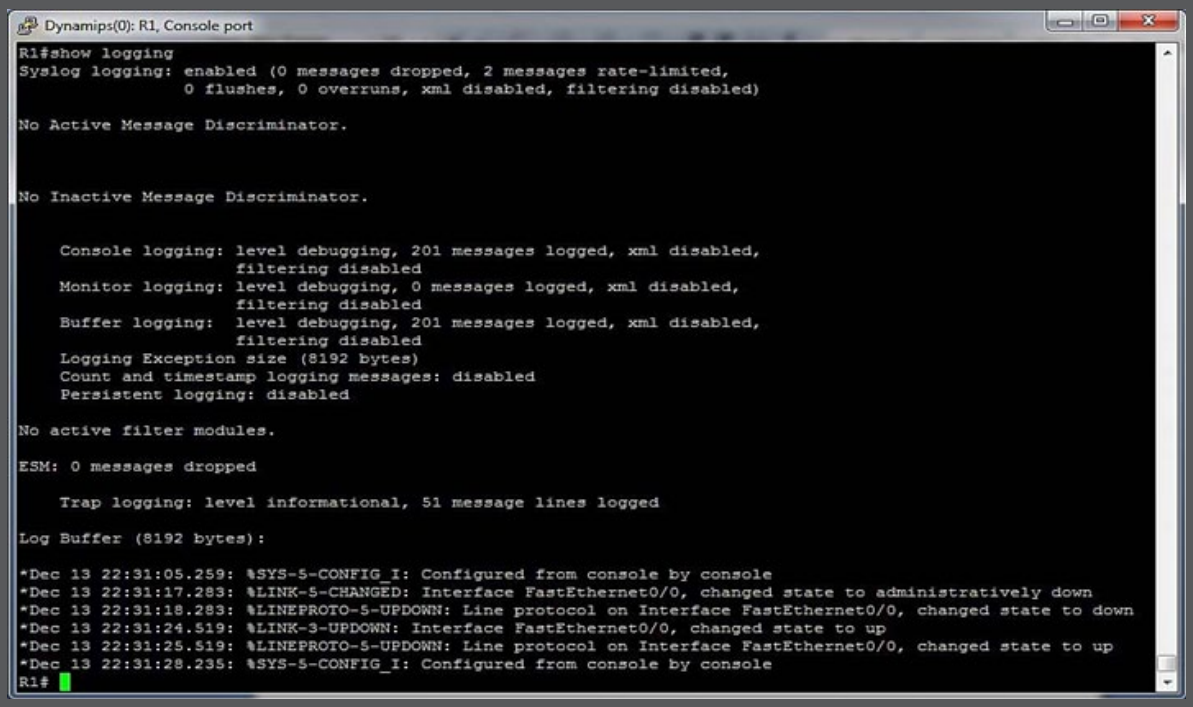
show ip route :

أمر حيوي يستخدم من قبل كل مهندس يعمل على جهاز سيسكو هو show ip route، ويستخدم هذا الأمر لعرض المحتوى الحالي للجدول توجيه (Ip routing table). الشكل أسفله يبين طريقين (routes 2) مختلفين يوجدان داخل جدول التوجيه، واحدة عبارة عن شبكة متصلة (شبكة 24/192.168.1.0)، و الأخرى هي default static route وهي ترسل كل prefixes غير المعروفة إلى الجهاز الذي عنوانه 192.168.1.1.



show logging :

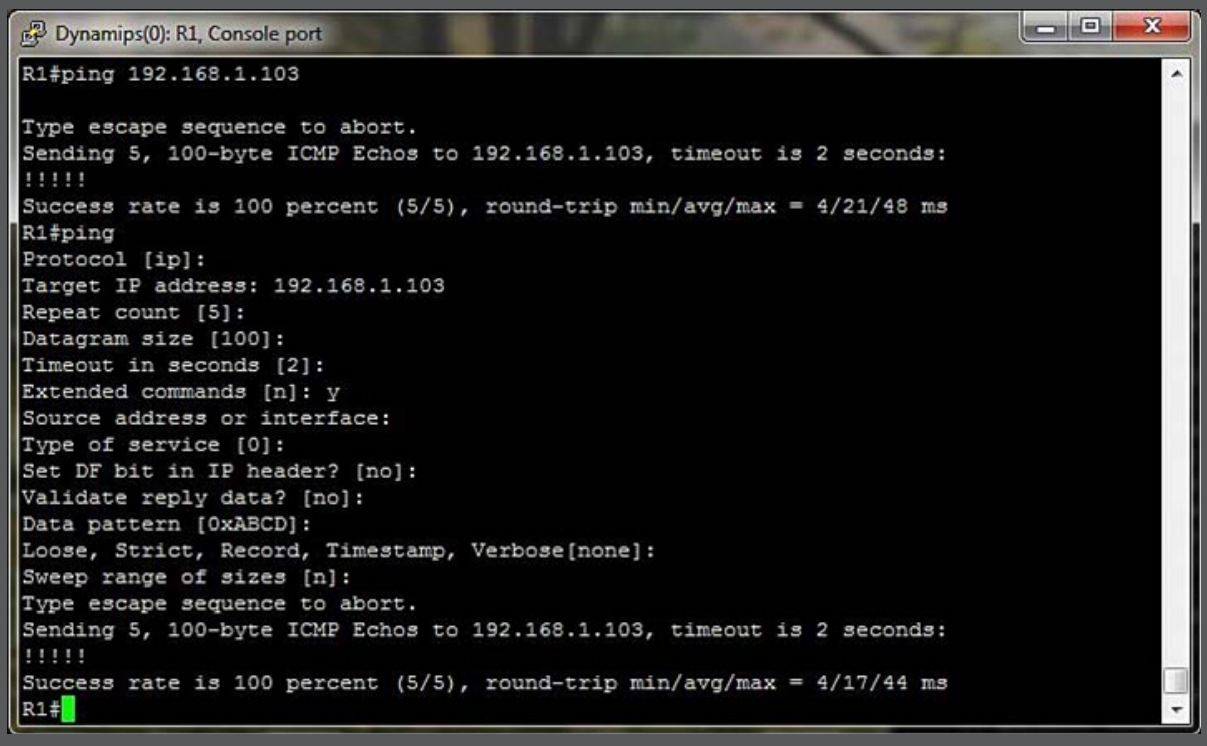
عندما يتم إعداد جهاز بـlogging ، يمكن استخدامه للتحقق من العديد من الاشياء المختلفة. يتم استخدام هذا الأمر للوصول إلى هذا log وعرضه للمراجعة. في الشكل أدناه ، تم إيقاف و تشغيل الواجهة لإظهار log الناتج عن هذه العملية.



ping :

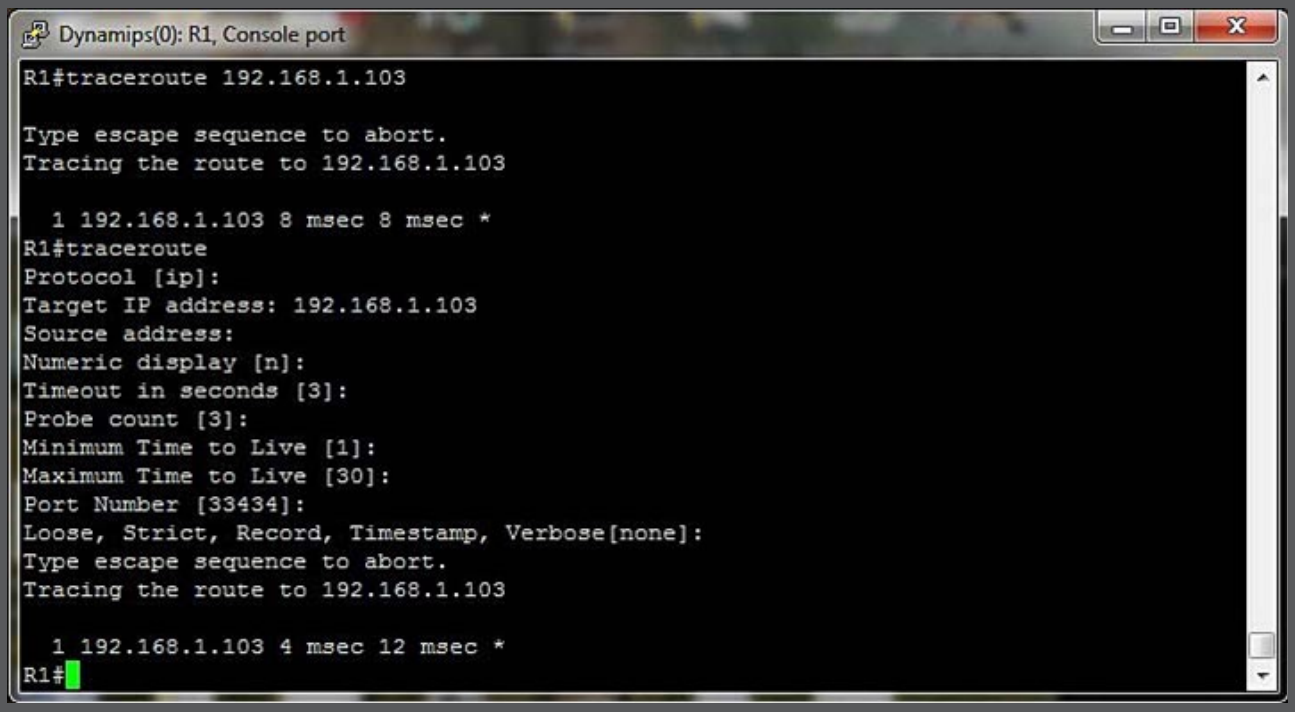
واحد من الآدوات الأكثر شعبية التي يتم استخدامها من قبل مهندسي الشبكة للتحقق من reachability هو أمرping . يتم استخدام أمر ping بإرسال مجموعة من خمسة حزمICMP إلى المرسل إليه والذي بدوره سيجيب بـ5 حزمICMP . و يمكن استعمال هذا الأمر مع عدد من الخيارات المختلفة من بينها تحديد count ، source interface ، حجمtimeout، datagram و Type of Service (ToS)...

تشمل الأمثلة كما هو مبين في الشكل تحت basic ping بدون خيارات إضافية نحو الوجهة 192.168.1.103 وصيغة ping موسعة (أيضا باستخدامdefault parameters).`



traceroute :

واحد من الآدوات الأكثر شعبية التي يتم استخدامها من قبل مهندسي الشبكة للتحقق من reachability هو أمرping . يتم هذا الأمر هو واحد من الأدوات التي تستخدم عادة من قبل المهندسين للتحقق من تشغيل الشبكة. فهو يقوم بإرسال عدد من الحزم لتحديد المسار من المصدر إلى الوجهة، والتي تتم من خلال الاستفادة من وظيفة TTL (Time to Live)الذي يوجد فيIP header . يسمح للمصدر بتحديد عدد «القفزات(Hops) » التي لا يسمح للحزمة عدم تجاوزها قبل أن يتم عمل drop لها. الشكل أسفله يعمل tracroute على host محلي وهو يبعد بـhop واحد فقط.



مرادفات هذه الأوامر في نظام تشغيل شركة الهواويVRP :

Cisco IOS	Huawei VRP
show ip interface brief	display ip interface brief
show interface	display interface
show ip interface	display ip interface
show ip arp	display arp all
show ip protocols	display ip routing-table protocol
show ip route	display ip routing-table
show logging	display logfile
ping	ping
traceroute	tracert

هناك عدد من الأوامر المختلفة التي يمكن استخدامها على جهاز سيسكو للتحقق من العمليات، الأوامر التي تطرقنا لها في هذه المقالة هي بعض من أبسط الأمور التي يتم استخدامها تقريبا من قبل كل المهندسين على أجهزة سيسكو في معظم الحالات. خذ الوقت للتحقق من هذه الأوامر على جهاز سيسكو (أوGNS3)؛ أيا منهم لن يؤثر على العمليات التي يقوم بها الجهاز، وسوف يوفر لك تجربة للتعلم . وبهذا نكون قد انتهينا والسلام عليكم و أتمنى أن ألقاكم قريبا إن شاء الله.

شهادة شكر وتقدير

تتقدم إدارة موقع

NetworkSet

First Arabic Magazine for Networks

بالشكر والتقدير للمهندس العماني

خالد عوض

لمساهمته معنا في المجلة ولتبنيه التحرير في قسم كتاب أعجبني
ولأسلوبه الأحترافي في أختيار مقالاته فجزاه الله عنا كل خير

مؤسس ومدير موقع NetworkSet
المهندس أيمن النعيمي

2012 / 3 / 30

حلّق في آفاق الوايرلس مع 802.11 n

لم يكد المصنعون يعلمون بوجود معيار جديد IEEE 802.11n-2007 للشبكات اللاسلكية حتي تهاتفوا علي draft في نسخته التجريبية تصنيع أجهزتهم طبقا لهذا المعيار حتي أنك لو تابعت تاريخ هذا المعيار ستجد أن الأجهزة قد سبقت اقرار nالتي صنعت مدعمة 802.11 IEEE 802.11n-2009 المعيار النهائي

و لا عجب في ذلك فبمجرد أن أطلق الإصدار النهائي منه أو اشرف علي الإصدار حتي قامت صاحبة الشهادات اللاسلكية CWNP مؤسسة المرموقة بدمج هذا المعيار و اختتمت به و ذلك كباب كامل CWNA منهجها الرائع يختص بهذا الأمر

الأمر بالفعل كان مغريا ففي الوقت الذي تنقل فيه شبكات الإيثرنت بياناتها بسرعة بسرعات 100/10 Mbps 802.11 نجد معيار nفإننا الأمر الذي جعلت Mbps يحلق بالشبكات اللاسلكية فوق قفار الإيثرنت و بسرعة تصل الي 300 النظرة للشبكات اللاسلكية تتغير من حيث كونها شبكات بطيئة نوعا ما

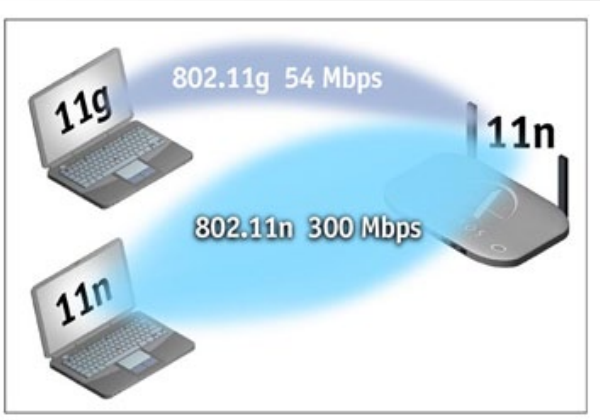
بتطويره عبر 11 نسخة تحريبية تسمي IEEE و لقد قم معهد مهندسي الإلكترونيات و الكهرباء قد nعلي مدي سنوات يظنها البعض بدأت من 2007 و انتهت في 2009 الا ان تاريخ 802.11 draft في High-Throughput Study Group (HTSG) بدأ قديما في 2002 عند انعقاد اجتماع مجموعة لمناقشة أمر زيادة انتاجية الشبكات اللاسلكية و لازالو حتي اليوم يطورون فيه رغم ظهور IEEE في اكتوبر 2009 published version النسخة النهائية

802.11 a/b/gيتفوق هذا المعيار بنسخته القديمة بخمسة أضعاف مقدرة الشبكات اللاسلكية العادية و قناته الترددية يصل عرضها 40 Mb/s فالمعيار الإبتدائي له ظهر بسرعة نقل بيانات بمقدار 300 بالإضافة الي التحسينات التي فعلها في نقل الإشارة لمسافات أكبر Mhz

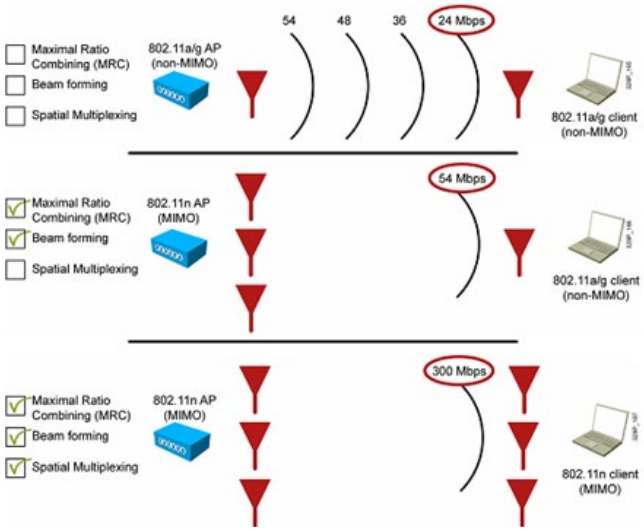
و الأكثر روعة من ذلك أن التعديل الذي تم عليه و الذي يعرف بـ IEEE 802.11n-2009 أو 802.11n amendment قد طور المعيار ليتصل سرعة الإتصال الي 600 Mbps و لولا تطور الإيثرنت لتصل سرعته الي 10 Gbps لأصبح خيار استبدال الشبكات السلكية بشبكات لاسلكية خيارا يجده البعض الزاميا و لكننا سنتكلم في هذا المقال عن معيار 802.11n ما قبل 2009 و لن يكون هناك فرق كبير سوي في السرعة التي وصلت حتي 600 Mbps

الغريب في هذا المعيار و الجيد و المذهل انه لم يعد يستخدم بروتوكولات RTS/CTS المستخدم في المعايير اللاسلكية العادية لأنه و ببساطة يعطي فرص جيدة جدا لجميع الأجهزة في الخلية للوصول الي الأكسس بوينت بدون التواجد في قائمة الإنتظار حيث شاركت الإيثرنت في خاصية full duplex فلم تعد بيات الشبكات اللاسلكية بحاجة للإنتظار المرسل كي يستقبل أو المستقبل كي يرسل بل من لديه بينات سيرسلها في أي وقت و ستصل بأسرع مما تتصور.

و مع هذا فإن هذا البروتوكول مطور لكي يتوافق مع هذه المعايير حيث أنه يتميز بوجود خاصية protection mechanism التي تميز معير 802.11g و الذي يستطيع من خلاله جعل الأكسس بوينت الذي يعمل بمعيار 802.11n قبول اتصالات من أجهزة تعمل بمعايير 802.11b , 802.11g , 802.11a



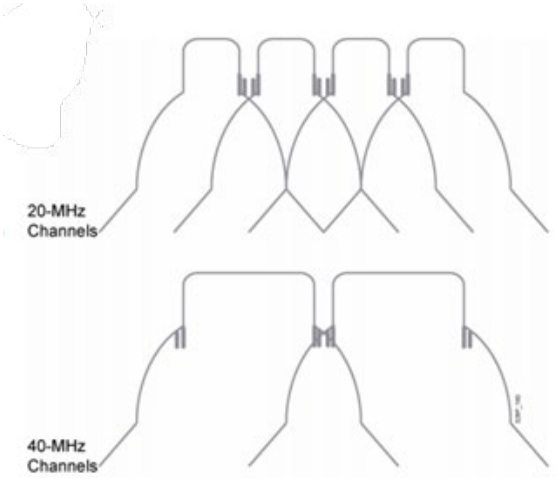
و تلخيصا لما سنذكره فإن هذا المعيار عند استخدامه للتراسل بين الأجهزة في جانب الأكسس بوينت و المستخدم فإنه يعالج القصور الناشيء عن اضمحلال data rate كلما زادت المسافة بين الأكسس بوينت و الجهاز ففي معايير 802.11a/g تضمحل data rate من 54 الي 48 الي 36 حتي تصل الي قمية 24 Mbps بينما في معيار 802.11n لا يحدث هذا الإضمحلال حيث أن تقنيات MRC و Beamforming و Spatial MUX و باستخدمها لتكنولوجيا MIMO عبر مصفوفة الهوائيات تقوم بمعالجة الإشارة لتحافظ علي قيمتها التي أرسلت بها حتي انك قد تلاحظ معدل تدفق للبيانات يصل الي 300 Mbps عند توفر هذه التقنيات جميعا



الكثير و الكثير قد طور من قبل هذا المعيار و الذي استخدم تقنيات لاسلكية و الكترونية واعدة جدا بدئا من MIMO و مرورا بـ MRC و Beamforming و نهاية بـ Spatial MUX

هذا المعيار أصبح من الشهرة و الكفاءة و الفعالية حتي أنه أطلق علي الشبكات التي تستخدمه - مستغنية عن كل المعايير السابقة – اسم الحقل الأخضر green-field و أنا – نادر - اسميها الواحة اللاسلكية

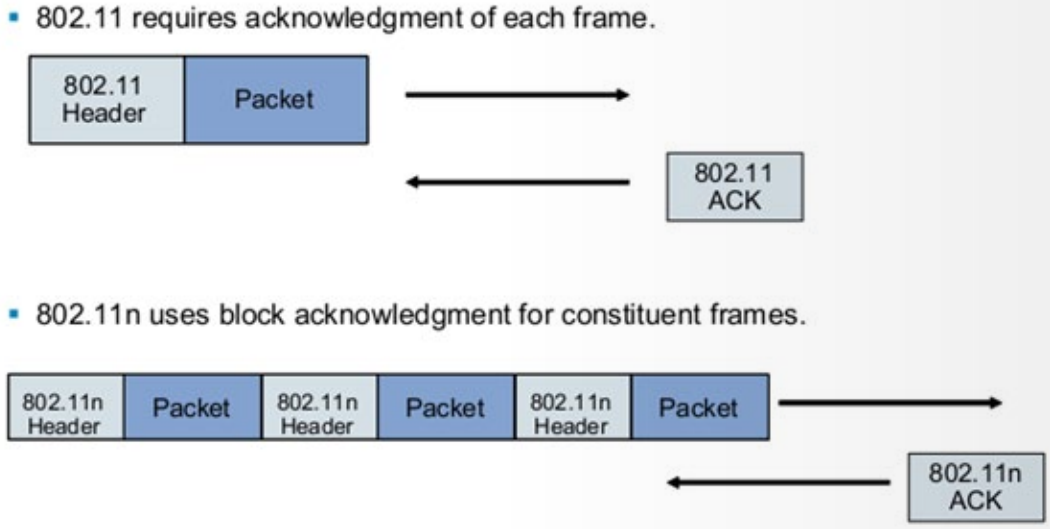
802.11n Channel Aggregation



يستخدم 802.11n قنوات بعرض MHZ 20 و 40 MHz و تعتبر القناة الترددية ذات العرض 40 MHz هي قناتين بعرض 20 MHz تم دمجهم و هاذ الأمر يجعل الأجهزة التي عمل بهذا المعيار قادرة علي بمعدلات نقل بيانات أعلي
و لكن عند استخدام هذا المعيار لعملية الدمج فإنه يفقد إحدي خصائصه المميزة و هي توافقيته مع معياري 802.11g و 802.11a
يتشابه 802.11n مع 802.11a و 802.11g في استخدامهم لتكنولوجيا التعديل الترددي OFDM الا أن 802.11n يزيد عدد subcarrier من 48 الي 52 في كل قناة ذات عرض 20-MHz و هذا يزيد أيضا من معدل نقل البيانات الي 260 Mb/s

802.11n MAC Efficiency

لكي يعمل بروتوكول 802.11 MAC بشكل طبيعي فإن أي شيء يتم ارساله خلال الوسط اللاسلكي يتم دائما التأكد منه بواسطة المستقبل عن طريق رسائل ACK acknowledgment و هذا الأمر يعطل قليلا الإرسال و الإستقبال حتي يتم التأكد من وصول المعلومة و هذا ما تم تخطيه في معيار 802.11n حيث أنه يقوم بتجميع aggregation صف كامل من الفريمات ثم يقوم بإرسالها كاملة و يطلب ACK لها جميعا و يسمي هذا الأمر block acknowledgment



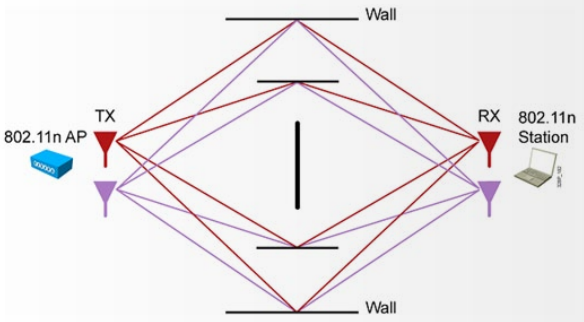
فمن المعروف في معايير 802.11a,b,g أنه يقوم بالإنتظار وقت استشعاري يسمي Distributed interface space DIFS قبل أن يسمح له بإرسال فريم كي يتأكد من خلو القناة و هذا أيضا مما يقلل من سرعة تدفق البيانات , يقوم أيضا 802.11n بتحسين سرعة تدفق البيانات بواسطة تقليل الفترات الزمنية الإستشعارية التي يحتاجها لإرسال الفريم و ذلك بإستخدام Reduce Interframe Space RIFS و هذا الأمر مفيد جدا في حال لو أنه لم يستطع تجميع الفريمات و ارسالها برسالة تأكيد واحدة فيقوم بإرسالها بالطريقة العادية للمعايير القديمة مع تقليل الفترات الزمنية بين كل فريم مرسل

MIMO – Spatial Multiplexing

يعرف 802.11n أيضا بـ MIMO و هو اختصارا لـ multiple-input, multiple-output و هو بروتوكول لاسلكي حديث صمم لزيادة سرعة و إنتاجية الشبكات اللاسلكية و تم اعتماده و استخدامه من قبل مؤسسة الواي فاي منذ صدوره في 2007 من مؤسسة مهندسي الإلكترونيات و الكهرباء IEEE

إحدي التقنيات التي يتم فيها استخدام أكثر من مستقبل و مرسل في نفس الجهاز و قد مكنت هذه التكنولوجيا الجديدة علوم الإتصالات خاصة الأجيال الحديثة لشبكات الجوال و شبكات الوايرلس 802.11n من زيادة تدفق البيانات عبر تمكين أكثر من مستخدم للإرسال و الإستقبال في نفس الوقت عبر محطة عمل واحدة التي قد تكون Access Point في الشبكات اللاسلكية أو Base station في شبكات الموبايل

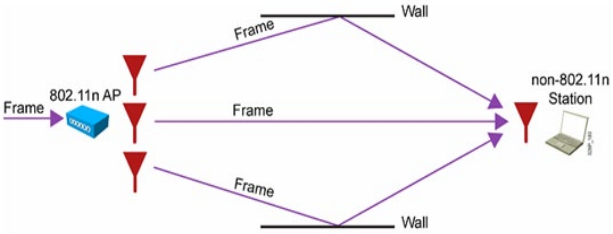
ليس هذا فقط بل ساعدت هذه التقنية شبكات الواي ماكس علي الإنتشار حيث أنها ركيزة اساسية لهذا النظام الشبكي و الذي يجمع بين خصائص شبكات الواي فاي كجهة تقدم خدمات انترنت و شبكات الموبايل الخلية التي تقدم الخدمة عبر محطات و أبراج لاسلكية تغطي المدن



و يعتبر MIMO أحد فروع تقنيات Multiplexing او MUX و هي ارسال أكثر من قناة ترددات لاسلكية و يتم ذلك عن طريق نقل الإشارات مع فصلها عن بعضها ترديا ثم استعادة القنوات المنفصلة عند مستقبل الإشارة و نسميه frequency division multiplex، أو بتخصيص تلك القناة المشتركة لعدة قنوات مختلفة لحمل المعلومات حيث تستخدم القنوات واحدة فواحدة زمنيا وهو ما يسمى time division multiplexing أو نرسل كل قناة بعد تشفيرها الي بتات معروفة للمرسل و المستقبل زمنيا ثم استعادة تلك الإشارات عند استقبالها و نسميه code division multiplexing و لكن تقنيتنا الحالية MIMO لا يصنف من ضمن هذه الفروع بل يصنف ضمن فرع آخر مغمور يسمي Spatial multiplexing حيث يتم ارسال أكثر من اشارة عبر نفس القناة و لكن بهوائيات متعددة أي أن الإشارات مفصولة مكانيا ولكل منها هوائي يخصها و هذا يفسر تسميتها بـ Spatialو تقوم هذه التقنية Spatial MUX بمضاعفة ثنائيا أو ثلاثيا أو رباعيا لمعدل نقل البيانات Data rate حسب عدد الهوائيات المستخدمة و يتم استخام ترقيم يساعدك علي فهم هذه التقنية هكذا مثلا 3x3x2 حيث يمثا الرقم الأول 3عدد هوائيات الإرسال و الثاني 3هوائيات الإستقبال و الثالث 2 لإشارات التدفق Spatial Stream

MIMO – Transmit Beamforming

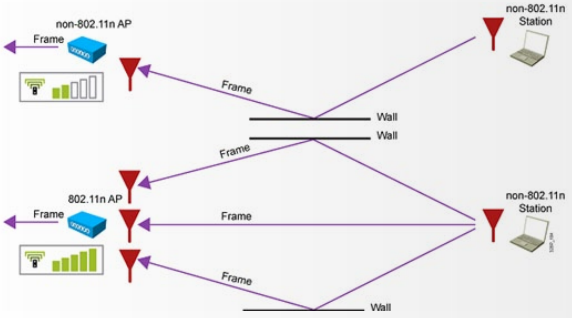
تكنولوجيا beamforming تستخدم عندما يتم التراسل بين جهازين أحدهما يستخدم معيار 802.11n + MIMO + Spatial MUX مع أجهزة لا تدعم هذا المعيار حيث أن الأجهزة التي تعمل مع تكنولوجيا MIMO ذات هوائيات متعددة علي عكس الأجهزة الأخوي التي تستخدم هوائي وحيد حيث يقوم هوائي المستقبل بتجميع اشارات هوائيات المرسل لضبط الفرق بين قيمها amplitude و طورها phase



و لا يتم هذا الأمر الا اذا تضمنت الإشارة معلومات عن نفسها و تسمي تلك المعلومات بمرجعية الإشارة feedback و هذه المرجعية ايضا لا تتوفر الا في الإشارات المرسلة من أجهزة تتعامل بمعيار 802.11n

MIMO – Maximal Ratio Combining

في جزء Transmit Beamforming تكلمنا عن طريقة تعامل الإشارة المرسلة من قبل أجهزة تدعم 802.11n و يتم استقبالها بوساطة أجهزة لا تدعم معيار 802.11n و هنا و مع تكنولوجيا MRC Maximal Ratio Combining سنتعرف علي العكس و هو كيفية ارسال الإشارة من أجهزة لا تدعم معيار 802.11n واستقبالها من أجهزة تدعم معيار 802.11n



كما قلنا فهذه التكنولوجيا تستخدم في مرحلة استقبال الإشارة من قبل الأجهزة التي تدعم معيار 802.11n اي أن هذه الأجهزة لها اكثر من هوائي و تقوم باستقبال الإشارات التي تصل للجهاز و تكون هذه الإشارات قد عانت بعضها من بعض التأخيرات نتيجة ظاهرة الإنكسارات و الإنعكاسات و غيرها و يقوم الجهاز بواسطة تكنولوجيا MRC بتحليل هذه الإشارات و تحديد قدرة كل منها و طورها ثم يقوم بجمعها معطيا مستوي عالي لها كما تري

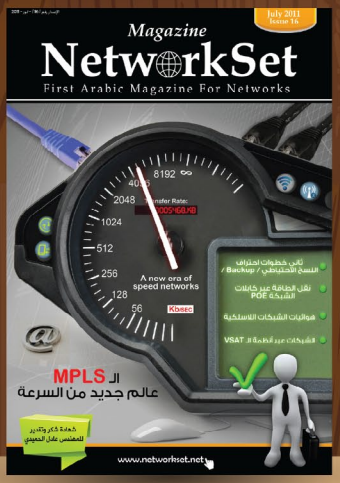
الهوائيات في 802.11n

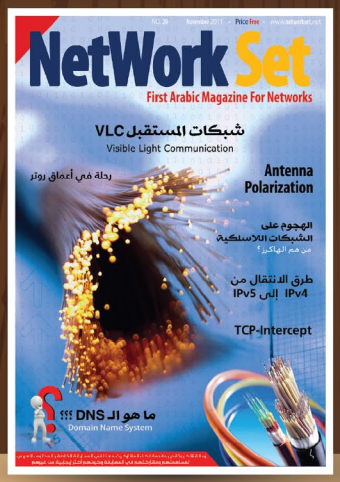
نظرا لإستخدام المعيار 802.11n لتكنولوجيا MIMO فإن ذلك يتطلب وجود أكثر من هوائي في الجهاز سواء كان هذا الجهاز أكسس بوينت أو كارت لاسلكي حيث يقوم كل هوائي بمعالجة البيانات ارسالا للمساعدة علي استقبال الإشارة بشكل أفضل و بمستوي أعلي

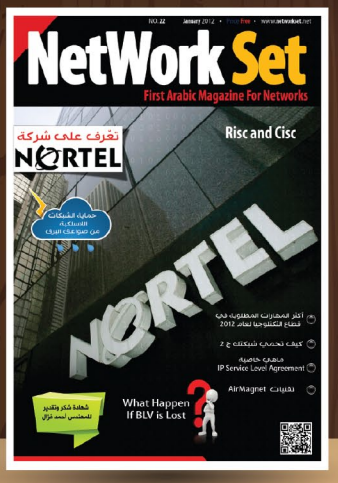
و هذه الهوائيات تختلف من جهاز لآخر من حيث العدد كلما زاد عدد الهوائيات في الأجهزة اللاسلكية فإن ذلك يزيد من قدرة الهوائي علي الإرسال و الإستقبال و يشار الي الأكسس بوينت بعدد هوائيات الإرسال و الإستقبال به فيطلق مثلا علي الأكسس بوينت 3x3 three by three عند استخدامه لثلاث هوائيات استقبال و مثلها ارسال و هناك أجهزة 2x3 كما الحال في الأكسس بوينت من نوع Cisco 1250 و تعتبر أجهزة اللابتوب التي تعمل كروتها اللاسلكية علي معيار 802.11n من فئة الأجهزة 2x2

تستطيع أن تميز الأجهزة التي تعمل طبقا لهذا المعيار بواسطة وجود هذه الهوائيات و ان كان الأمر ينحو نحو استخدام هوائيات مدمجة في الأجهزة كما هو الحال مع الأجهزة الخلوية و لذلك فما عليك الا أن تبحث عن وجود هذا الشعار علي غلاف الأجهزة أو مطبوعا عليها

Network Set Magazine Gallery







الـ Honeypot
مصيدة للهاكرز

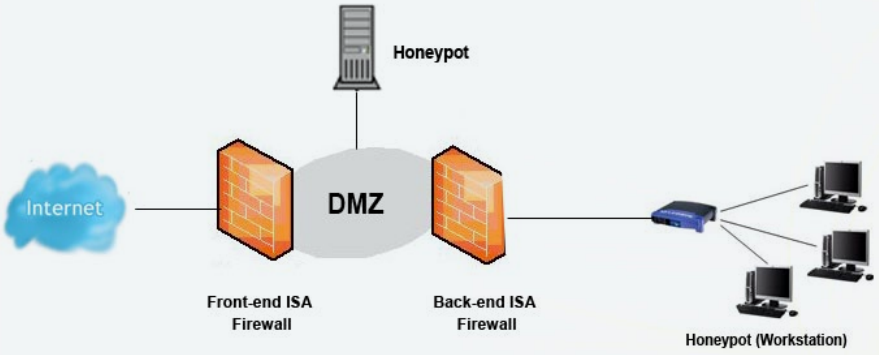
في الأونة الأخيرة وخوصوصا الفترة عام 2011 – 2012 ، شهد شبكة الأنترنت العنكبوتية تزايداً شديداً في عدد الإختراقات . ليس ذلك فحسب ، بل كانت تلك الإختراقات عنيفة ومخيفة فقد إستخدم الهاكرز فيها طرقاً وأساليب متقدمة لم تكن متوقعة من قبل المؤسسات التي تحصن أنظمتها بالأجهزة والبرمجيات المتقدمة في الأمن والحماية . وقد إتفق خبراء الأمن والحماية بأنه لا يمكن وقف مخترقي الأنظمة بنسبة 100٪ بل يمكننا الحد من عمليات الإختراق وإصطياد المخترقين . فقد قام أحد مجموعة من الأشخاص بإبتكار مشروع نظام أمني جديد يهدف إلى التقليل من خطورة الإختراقات وخداع الهاكرز وأسموه Honeypot . فقد أتينا لكم في هذا المقال لنسلط الضوء على هذا النظام الأمني وما فائدته وكيف يعمل .

نظرة عامة على الـ Honeypot :

الـ Honeypot هو عبارة عن نظام صمم للشبكات بهدف خداع الهاكرز عند محاولتهم لإختراق الشبكة والأنظمة . ويأتي هذا النظام على شكل سكربتات يتم برمجتها على أحد أجهزة عملاء الشبكة . وكذلك يأتي كنظام تشغيلي متكامل يثبت على جهاز حاسب الالي ليعمل كسيرفر في الشبكة وذلك لتتبع الهاكرز وخداعهم . والجدير بالذكر هنا ، أن هذا النظام لا يحل محل أجهزة الحماية مثل الـ Firewall وغيرها وإنما يرتبط بها لزيادة مستوى الحماية .

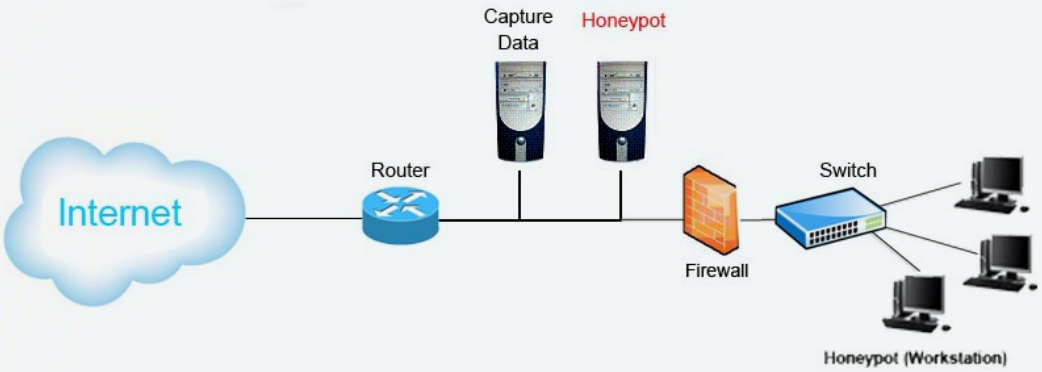
كيف يتم عمل الـ Honeypot على الشبكة ؟

كما ذكرنا لكم سلفا بأن هذا النظام يعمل كجهاز client وايضا كسيرفر في الشبكة ويكون عادة موصول في منطقة DMZ والتي يكون فيها Firewall كما هو واضح في الصورة التالية :



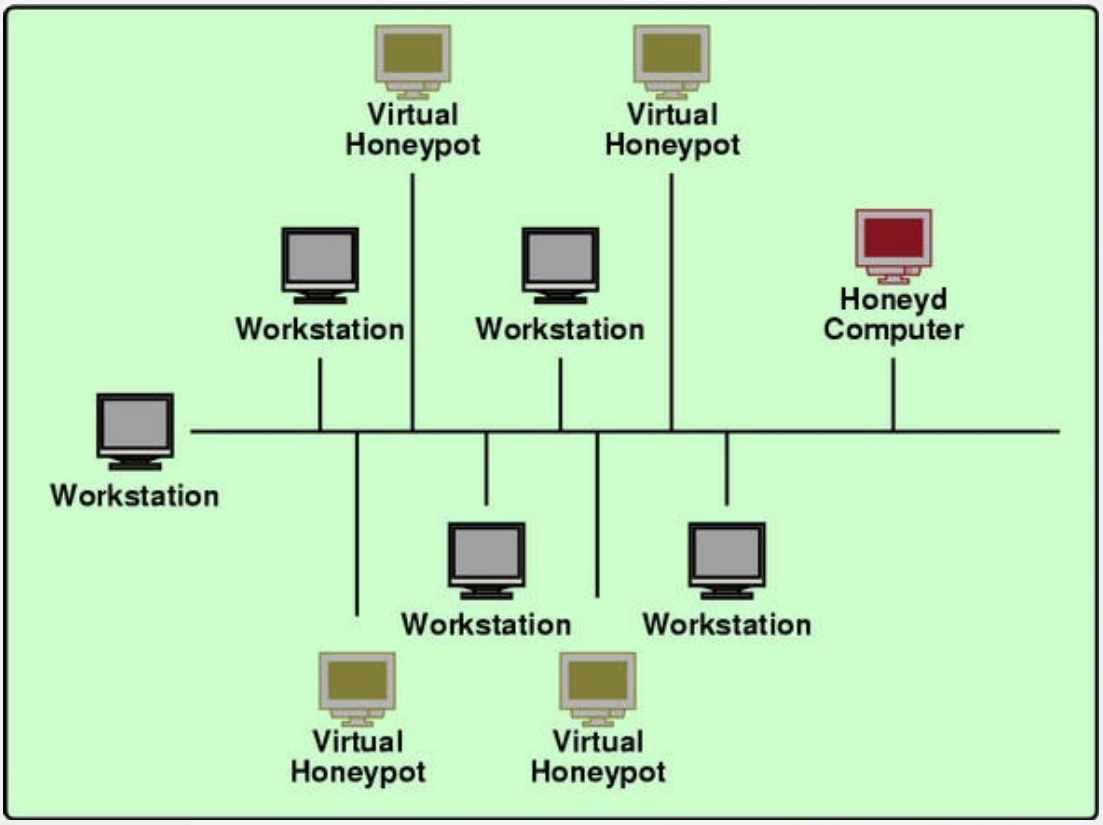
حيث أن هذا النظام في حالة الـ Client او Workstation يثبت كسكربت أو سطور برمجية يتم برمجتها في نظام لينكس ويسمى هذا النوع Low Level Interaction . أما عندما يعمل الـ honeypot في وضعية السيرفر ، فإنه هنا يكون كنظام تشغيلي متكامل أو Operating System ويتم تركيب هذا النظام على السيرفر كحال تركيب السيرفرات الأخرى ويسمى الـ honeypot من هذا النوع بـ High Level Interaction .

بعد التعرف لهذا النظام ، نود أن نخبرك بأن هذا النظام إختراقة أسهل من إختراق الـ Firewall .
ولعلك تتسأل !!
إذن ما الحكمة من إستخدام النظام إذا كانت حماية أضعف من الجدار الناري ؟؟
سنجيب على سؤالك هذا بوضوح من خلال الصورة التالية والشرح الذي يليها :



ركز معنا من خلال الصورة. عندما يأتي المهاجم لينفذ هجومة ، فإن هجومه سيكون على الـ honeypot أولا لأنه أسهل من إختراق الجدار الناري كما ذكرنا . والحكمة من ذلك لو تأملت في الصورة ستجد أن هنالك جهاز Capture Data قبل الـ honeypot . فعندما يخترق المهاجم الـ honeypot فإن جهاز الـ capture data يقوم بتسجيل عمليات الإختراق التي يقوم بها المهاجم ويحلل الـ packets او حزم البيانات الورادة من وإلى المهاجم . ومن هنا فإن تحركات المهاجم والحيل التي يستخدمها قد تم تسجيلها. ويستفاد من تسجيل عمليات المهاجم لمراجعتها عند حدوث تحقيقات في الجرائم الرقمية ليتم الكشف عن المهاجم .
لهذا فإن الـ honeypot هو مصيدة وفخ للهاكرز . حيث يظن الهاكرز بأنه إختراق الأنظمة ولكن الحقيقة قد أخترق أنظمة وهمية وهي الـ honeypot وقد تم إصطياده وكشف أسرار الشريرة في إختراق الأنظمة .

لكن ماذا لو كان لدينا شبكة صغيرة لا تحتوي على سيرفر ولا جدار ناري ؟؟ فهل يمكن حماية شبكتنا بهذا النظام ؟؟
للإجابة على سؤالكم هذا فإننا نوضح لكم بالصورة التالية :



من خلال المخطط ، فإنك تلاحظ أن كل جهاز حاسب على الشبكة مركب عليه نظام honeypot عن طريق برامج الـ virtualization والتي بدورها ان تركب أكثر من نظام وهمي على حاسبك . ومن هنا فأنه عندما يحاول المهاجم الهجوم على الأجهزة فإنه سيقصف نظام honeypot الوهمي ولن يلحق الضرر بالحايب الحقيقي . وإن لم ترغب بإعداد النظام ليكون وهمي فيمكنك إستخدام سكربتات معينة لعمله كـ low level interaction والذي تحدثنا عنه قبل قليل .

وما يهمنا في هذا الموضوع هو أن نتوخى الحذر عند تركيب الـ honeypot . فيجب أن نعرف الأمور التالية لتركيبه بطريقة فعالة تبعدنا عن الضرر وتنقذنا من شر الهاكرز .

- يجب أن تعد الـ honeypot ليظهر على أنه نظام حقيقي او سيرفر حقيقي حتى يشعر الهاكرز بالسعادة ويقضي وقتا أطول في التلاعب بالنظام . وقضائه لوقت أطول يساعدنا على جمع قدر أكبر من المعلومات عنه وعن أساليب وطرق إختراقه .

- يجب أن تعد الـ honeypot بطريقة دقيقة بحيث لا يسمع للمهاجم أن يتجاوز إختراقة لجمع معلومات حقيقية عن بنية الشبكة الخاصة بك .

- من خلال المخططان السابقان ، لاحظ أن الجدار الناري أو Firewall مرتبط بالـ Honeypot وذلك لأن الجدار الناري يقوم بتسجيل ما يحدث لنظام الـ Honeypot في سجلات خاصة ويرسل تقرير لمدارء الشبكة بأن احد المهاجمين اخترق النظام . ويمكنك أيضاً تتبع المهاجم وتحركاته عن طريق أدوات معينة تسمى Sniffing Tools والتي بدرها تحليل الـ packets لا تعبر من وإلى المهاجم وذلك لمعرفة الأدوات التي يستخدمها في الإختراق والمنافذ التي يدخل منها إلى الشبكة .

أما لمن يتسأل عن تركيب هذا النظام ومن أين الحصول عليه ، فإننا نجيب عليك بأن هنالك عدة نسخ منها ما يركب على Physical Machine او جهاز حقيقي ومنها ما يمكن تركيبه على Virtual Machine او حاسب وهمي من خلال تقنية Virtualization . وهذه أسماء بعض التوزيعات المتوفرة :

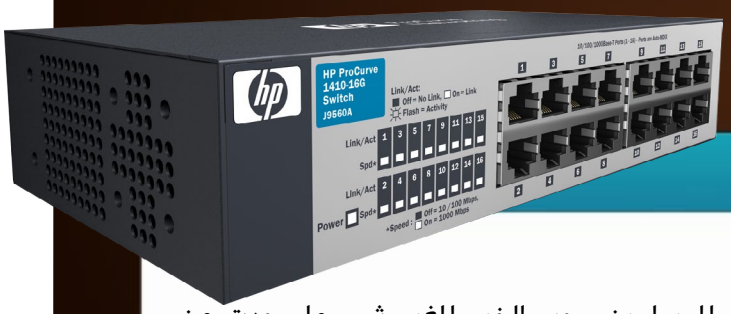
Tripwire و CyberCop Sting و Man Trap .

وختاما لكم فقد أسعدنا الحديث معكم عن هذا الموضوع الشق والذي تفتقر مصادرنا العربية بمعلومات عنه وإننا ننصح مهندسي أنظمة الحماية ومدراء نظام لينكس أن يتطلعوا لهذه النظام لما له من دور فعال في تطوير الحماية ورفع مستواها . وإذا أردت مراجع مميزة تتحدث عن هذه النظام فإننا نوصيك بأن تقتني هاذان الكتابان :

كتاب :
Honeypots: Tracking Hackers

كتاب :
Virtual Honeypots: From Botnet Tracking to Intrusion Detection

مقدمة عن سويتشات شركة HP



دفعني حبي لديني وللمسلمين وحب الخير للغير ثم ما وجدت من المهندس أيمن النعيمي من إجتهاد في نفع الامة العربية الكريمة دفعني ذلك الى المحاولة في كتابة مقال عربي تخصصي أتمنى من اللّه أن تكون خالصه لوجه الكريم.

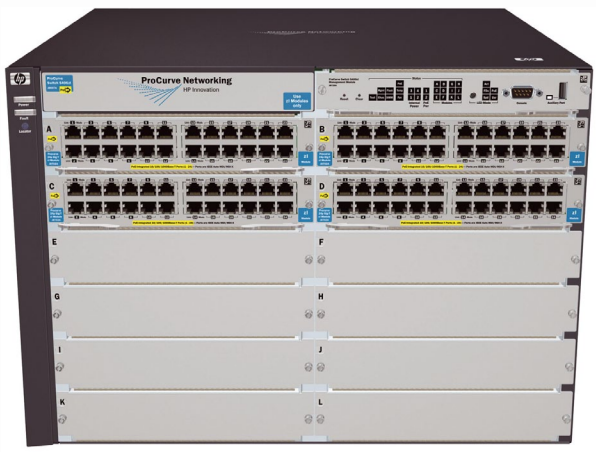
بدأت سويتشات HP Procurve بالظهور بقوة على الساحة حتى تنافس شركة سيسكو وجونيبر في مجال السويتشات وكما تعرفون فقد قامت شركة HP بشراء شركة 3com وقامت بعدها بتغيير جميع أسماء المنتجات التى تقوم الشركة بإنتاجها من HP Procurve الى HP-N وحرف N يرمز الي Networking

ومن أشهر السويتشات التي يتم إستخدامها في المشاريع الكبرى :

- HP Procurve 3500 yl :

http://h17007.www1.hp.com/us/en/products/switches/HP_3500_yl_Switch_Series/index.aspx?jumpid=reg_r1002_usenV

- HP Procurve 5400 zl:



http://h17007.www1.hp.com/us/en/products/switches/HP_5400_zl_Switch_Series/index.aspx

• HP Procurve 8200 zl :

http://h17007.www1.hp.com/us/en/products/switches/HP_8200_zl_Switch_Series/index.aspx

طبعا هذا السويتش ينتمي الى Modular Chassis switches يعني انه قابل لاضافة Modules
مايميز سويتشات شركة HP عن باقي الشركات المنافسة سواء سيسكو أو جينيبر.

1. سويتشات HP تعطي أسعار منافسة لسويتشات سيسكو
2. سويتشات HP تعطيك على كل السويتشات Life Time Warranty.
   يعني ضمان مدى الحياة ويكون ضمان استبدال وأظن هذه ليست موجود في سيسكو.
3. سويتشات HP ذات كفاءة عالية وتعطيك مميزات سيسكو .
4. جميع سويتشات HP تعمل Layer 3 وهذه ميزة كبيرة .
5. هناك شخص أعرفه جيدا يعمل في مشروع كبير به حوالي 3000 HP Procurve Switch

أما بالنسبة لنظام التشغيل الخاص بسويتشات HP فهو Software Image ويحتوي فقط علي :

- Operational Mode
- Configuration Mode

وهو سهل التعامل معه مثل سيسكو اذا نسيت اي امر فيمكنك وضع علامه استفهام لمعرفة الامر التالي وكذلك يمكنك ضغط Tab لتكمله الامر .
وسوف أقوم باستعراض بعض أوامر سويتشات HP وكيف أنها قريبة جدا من سيسكو.

```
HP3500> enable
HP3500# configure terminal
#(HP3500 (config
```

To view possible copy command options, enter the following:

```
? HP3500# copy
flash
running-config
startup-config
tftp
? HP9300# copy flash
Tftp
```

To view all available commands at the user EXEC level, enter the following or press TAB at the User EXEC CLI level:

```
<HP3500> ? <return
enable
exit
fastboot
ping
show
stop-trace-route
traceroute
```

وهذه طريقة تخصيص IP Address on Switch

```
255.255.255.0/HP3500(config)# vlan 1 ip address 10.28.227.103
24/HP3500(config)# vlan 1 ip address 10.28.227.103
```

To Save Configuration :

```
HP3500 (config)#write memory
```

To Delete Configuration:

```
HP3500 (config)# erase startup-config
```

Other Commands

```
:Show current firmware revision
HP3500>show version
.Show memory and CPU usage info
HP3500>show system
:Show configuration
HP3500>show running-config

:Show LLDP/spanning tree configuration
HP3500>show lldp config
HP3500>show spanning-tree
:Reboot
HP3500>reload
```

هذه مقدمة عن سويتشات شركة HP وإن شاء اللّه سوف نستمر في المقالات القادمة في تناول سويتش معين لدراسته باذن اللّه

كتاب أعجبني

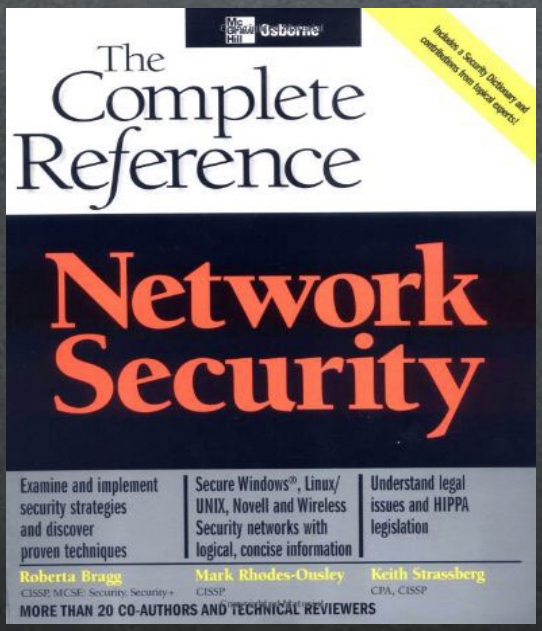
إن من أحد الأمور المهمة التي ننظر إليها عند البحث عن الكتاب المميز والغني بالمعلومات ، أن نبحث عن المؤلف المتميز الذي يبذل جهدا شاقاً لإخراج كتابه بالصورة التي تناسب القاريء . ومن هذا الأساس فقد إخترنا لكم اليوم أحد الكتب الرائعة والممتعة والذي إشترك فيه 29 مؤلف متعددي الخبرات وواسعي العقول في مجالهم . فمنهم الخبير في مجال الشبكات ومنهم من في مجال الإتصالات . وهنالك أخرين متخصصوا في البرمجيات وقواعد البيانات . جمعوا جزءً من خبرتهم الواسعة والتي تصل لبعضهم أكثر من 25 عاماً . ووضعوا تلك الخبرات في كتاباً واحد ليكون مرجع لمتخصصي الأمن والحماية في الشبكات

إسم الكتاب :
Network Security:
The Complete Reference

تأليف :
خلاصة خبرة 29 مؤلف تقني خبير

اللغة : الانجليزية

عدد الصفحات : 815 صفحة



أما عن محتويات هذا الكتاب ، فهو مقسم إلى 6 أبواب وكل باب مقسم إلى عدة فصول وذلك كتالي :

الباب الأول :

يتحدث عن أساسيات الحماية في الشبكات والإستراتيجيات والسياسات الأساسية المتبعة في الحماية .

الباب الثاني :

يتحدث عن الـ Access Control بشكل عام ويفصل فيها ليتحدث عن العناصر التي يجب أن نطبقها فيزيئا لحماية الأنظمة . كذلك في هذا الباب يوجد فصل خاص يتكلم عن الصلاحيات والتوثيق . وفصل أخر عن كيفية حماية البيانات . وفصل ثالث عن كيفية إدارة الحماية .

الباب الثالث :

هذا الباب مميز جدا في الكتاب ومليء بالمعلومات حيث تحدث المؤلفيين فيه عن أجهزة الأمن والحماية ، الجداران النارية ، الحماية في شبكات VPN ، أجهزة الحماية في الشبكات اللاسلكية ، أجهزة IDS وعن دور الأنظمة والسيرفرات في حماية الشبكات.

الباب الرابع :

يتحدث عن انظمة التشغيل وما يتعلق بها في الجانب الأمني فقد ركز المؤلفيين على نظام ويندوز ولينكس ويونكس وكذلك نظام نوفل .

الباب الخامس :

يتحدث عن حماية البرمجيات وقواعد البيانات . وتم تسليط الضوء هنا على الكثير من الأمور مثل SQL و لغة الجافا ودورها في برمجية أنظمة الحماية . كذلك تحدث المؤلفيين عن الحماية فيما يتعلق بالويب.

الباب السادس :

يتحدث عن الإستجابة ضد الأضرار من نسخ إحتياطي والحماية من الفيروسات . كذلك تطرق المؤلفيين إلى قضية حماية الحسابات وكلمات المرور . وذكروا احد المواضيع المتقدمة وهي التحليل الجنائي في الجرائم الرقمية .

الخلاصة :

هذا الكتاب موجه لمن يحب مجال الأمن والحماية في الشبكات ولمن يريد أن يطلع على أهم الأمور الواجب معرفتها غب أمن الشبكات بشكل عام . فهو مرجع ممتاز ورائع جداً وغني بالمعلومات فقد أبدع فيه المؤلفون وتبقى زأنتظروا منك تستمع بقرائة ما كتبوه لعلك تصبح يوما مثلهم .

MIGRATION OR UPDATE ? IS YOUR CHOICE

فى يونكس AIX التابع لشركه IBM فانه فى الغالب يكون هناك اصدار جديد تقريبا كل اربع او خمس سنوات يتخللها العديد من التحسنينات التى يتم ادخالها على الاصدرات الخاصه بها ودعنا نضرب مثال على ذلك .

فهناك مثلا الاصدار 5 ,6,7 ويتم تسميتهم كالتالى 5L or 5 level اى الاصدار الخامس بكل ما يحتويه من اصدارت فرعيه مثل 5.1 , 5.2 and 5.3 فهولاء الثلاثه مجتمعيت يكونوا 5L وهكذا ايضا بالنسبه للاصدار 6 فهو يشمل 6.1, 6.2 , and 6.3 .

هناك تحديثات ايضا تخلل كل اصدار فرعى من هذه الاصدرات تعرف باسم Fix back والتى هى عباره عن fixes خاصه بحل بعض المشاكل او bugs الموجوده بنظام التشغيل وهناك ايضا ما يعرف ب maintenace level وهو مثل التحديثات لنظام التشغيل updates الفعليه لهذا النظام.

لتقريب المثال دعنا نضرب مثل هذا المثال على الويندوز فهناك الاتى :

1 - اصدارات كبيره مثل XP , VISTA , and 7 فهى تمثل مثل 5L , 6L ,and 7L فى اليونكس التابع IBM .

2 - هناك تحديثات updates مثل service pack1 service pack 2 , وهذا تمثل هنا 5.1 , 5.2 and , 5.3 فهى تحديثات تضاف الى نفس النسخه من نظام التشغيل لتحديث امكانياته .

3 - وهناك ايضا التحديثات العاديه التى تقوم انت بتزيلها من موقع ميكروسوفت او automatically وهى هنا تمثل فى اليونكس Maintenace level فنحن ايضا نستطيع انزالها من على موقع IBM بدون اى مقابل مادى .

4 - هناك ايضا بعض التحديثات الخاصه بمشكله معينه فى النظام bugs وهنا لحل مثل هذا المشاكل نقوم بتحميل ما يعرف FIX وهو يكون عباره عن رقم يسمى APAR تبحث به فى موقع IBM الالكترونى وتقوم بتحميله وحل المشكله التى تواجهك .

وعندما تقوم بالتحديث عليك ان تقوم بمعرفه ما تريد تحديثه وهذا تستطيع معرفته من خلال ال command التالى oslevel والذى يحدد هل انت تحتاج الى تعديل فى ال version والذى بدوره يتكلف اموال واما ان يكون من خلال ال fix back فقط . ولتحديد maintenace level الذى تحتاجه فعليك بالامر التالى oslevel -r فستجد النتيجه كالتالى مثلا 6100-05 فهذا معناه التالى :

6 is the operating system version , 1 is the release of this 6 level , 0 is the modification level , 0 is the fix back level , 05 is the maintenace level .

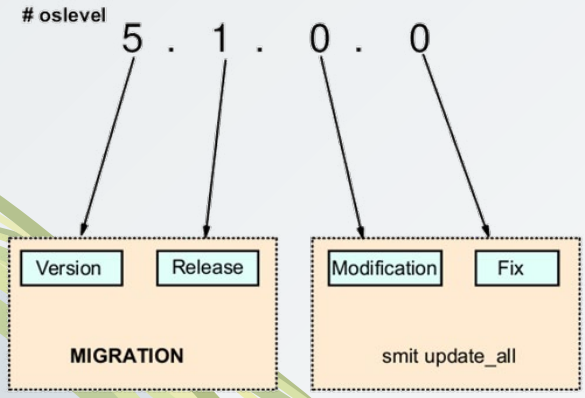
دعنا نضرب مثال على هذا :

- اذا اردت ان تقوم بتحديث نظام التشغيل من (5.1 to 5.2) فانت ستقوم بعمل migration اى انك تقريبا تتنقل من نظام الى نظام اخر لانه يقوم ببعض التعديلات فى System Libraries التى يعمل عليها .

- اذا اردت ان تقوم بتحديث نظام التشغيل من 5L to 6L فانت ايضا ستحتاج الى القيام بعمليه migration

- اما اذا اردت ان تقوم بتحديث نظام التشغيل من 5.3.0.2 الى 5.3.0.4 فانت فى هذه الحاله ستقوم بانزال ال fix back المطلوب لهذه العمليه وتحديث نظام التشغيل .

- اما اذا اردت تعديل maintenance level من 005 الى 007 مثلا فانك هنا ستقوم بانزال maintenace package الخاص بهذا من موقع IBM وتسطيبها على نظام التشغيل من خلال smit update_all .



خطوات القيام بعمليه MIGRATION :

1 - فى هذه الحاله لابد اولا من تواجد الاسطوانه الخاصه بنظام التشغيل المراد تحديث النظام اليه وليكن مثلا 5.3 .

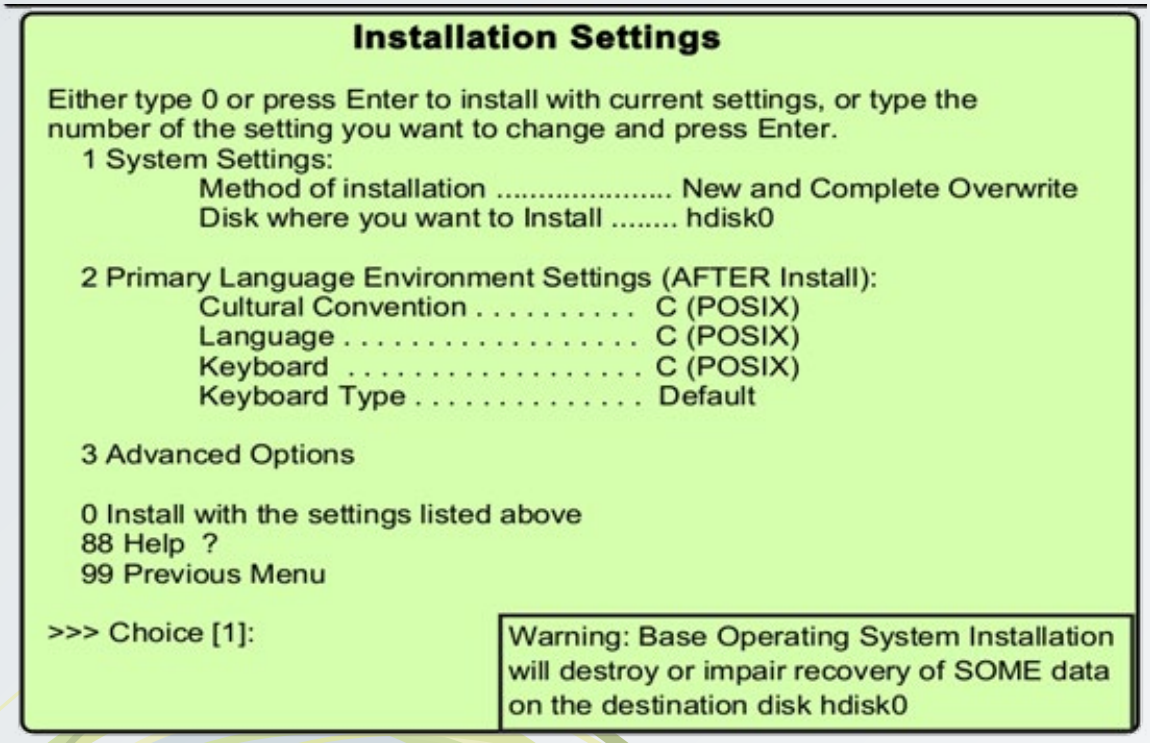
2 - نضع هذه الاسطوانه فى CD-Rom Driver والقيام بعمليه اعاده تشغيل من خلال command الاتى: shutdown –Fr .

3 - عند بدء عمليه اعاده التشغيل نضغط f5 او 5 تبعا للسيرفر لنقوم بالدخول الى maintenance mode .

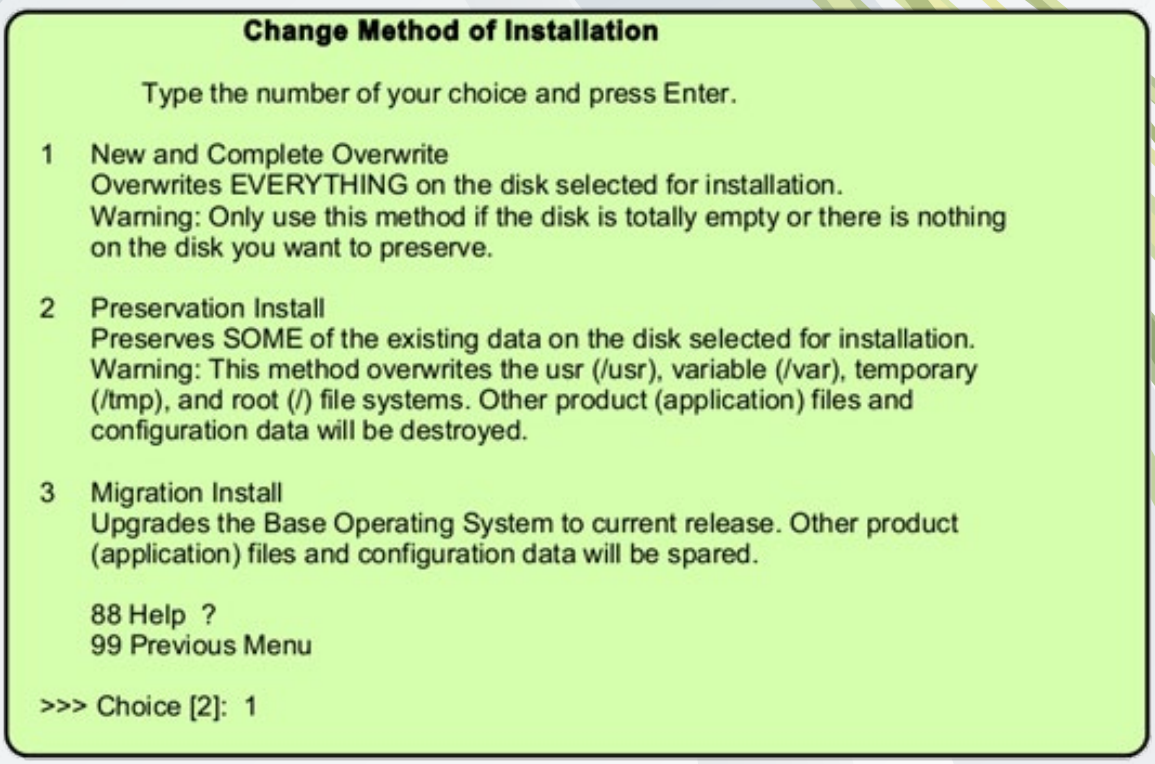
4 - نكتب رقم 2 حتى نقوم باختيار change/show installation setting and install كالاتى :

```
Welcome to Base Operating System
Installation and Maintenance

Type the number of your choice and press Enter. Choice indicated by >>>

>>> 1 Start Install now with Default Setting
    2 Change/Show Installation Settings and Install
    3 Start Maintenance Mode for System Recovery


    88 Help ?
    99 Previous Menu
>>> Choice [1]: 2
```

5 - ثم نقوم بكتابه 1 حتى نقوم بالتعديل فى كيفيه booting من الاسطوانه :



6 - ثم نكتب الرقم 3 حتى نختار migration install بدلا من الاختيار السابق New and Complete Overwrite وبالتالى تبدء عمليه التحديث :



وبذلك تكون قد بدءت عمليه migration اما للقيام بعمليه التحديث من خلال maintenance level فعليك القيام بالخطوات الاتيه :

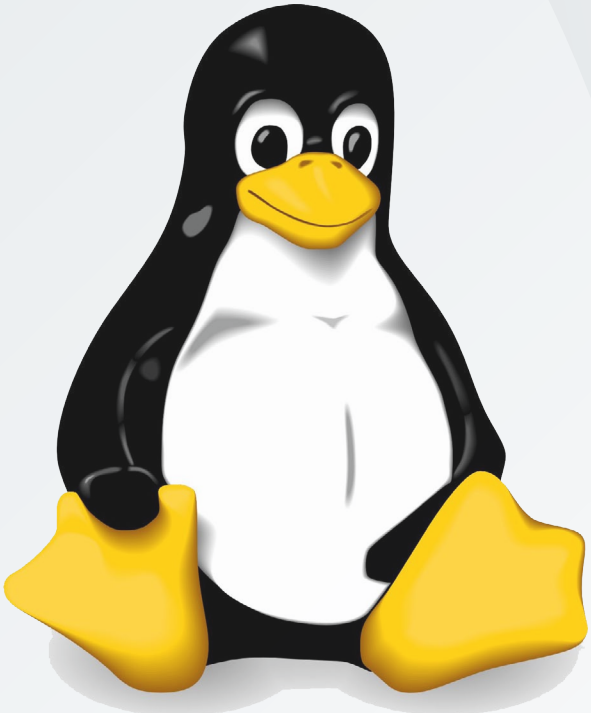
1 - تحميل ال Maintenance level من موقع IBM الالكترونى فمثلا لتحديث نظام التشغيل من 5.3 02 الى 5.3 04 فعليك بالذهاب الى موقع IBM وتحميل Maintenance level الخاص ب 5.3 04 ووضعه على اسطوانه .

2 - وضع الاسطوانه فى CD-ROM Driver والذهاب الى smit menu من خلال الامر التالى smit update_all .

3 - تحديد المكان الموجود به الاسطوانه كالتالى /dev/cd0 ثم عمل install لمحتويات هذه الاسطوانه .

4 - بعد تمام عمليه التنصيب قم بعمل reboot عن طريق الامر التالى shutdown –Fr .

5 - للتاكد من ان هذه الخطوه تمت بنجاح بقوم بكتابه الامر التالى oslevel –r ونرى النتيجه التى تظهر فيجب ان تكون 5.3-04 .



فهم علاقات الثقة
Understanding Trust Relationships

في البداية كلما تعمل تنفيذ لشبكة تحتاج لي اثنين وأكثر من AD DS Domain أنت أكيد في هذه الحالة ستكون تعمل بعلاقة الثقة Trust Relationships ، أو الثقة بشكل عام . وفي هذه الحالة يجب عليك تكون تعلم ومستوعب ما هي وظيفة وأعداد علاقات الثقة Trust Relationships

علاقات الثقة في نفس الـ Domain :

عندما الجهاز ينظم إلى الـ Domain ينشئ علاقة ثقة مع الـ Domain ، وتأثير هذه الثقة انه هذا الجهاز يسمح للمستخدمين يعملوا عملية التحقيق من أسم المستخدم وكلمة السر authenticated ليس من الجهاز المحلي من الـ (SAM) لكن عن طريق خدمة التحقيق تبع الـ Domain التي هي AD DS . والـ Domain Controller أيضا يسمح لعناصر الـ Domain لتستخدم من أجل تأمين موارد النظام . على سبيل المثال ، مستخدمين الـ Domain يضافوا إلى مجموعة تسمى Users Group وعن طريقها ممكن ان اسند للمستخدمين الصلاحيات للدخول على الجهاز Locally . أيضا حسابات المستخدمين والمجموعات في الـ Domain ممكن ان يضافوا إلى الـ ACLs على ملف أو مجلد أو طابعة على النظام . كل أعضاء الـ Domain لديهم نفس علاقات الثقة مع الـ Domain ، وهذا يجعل الـ Domain أن يكون مخزن وسيط للعناصر (المستخدمين والمجموعات) وكمان يكون خدمة وسطية تقدم عملية التحقيق من اسم المستخدم وكلمة السر (authentication)

علاقات الثقة مابين أكثر من Domain :

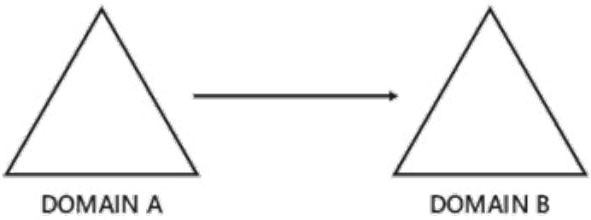
على نفس النمط السابق ممكن ان توسع مفهوم علاقات الثقة إلى Domain أخر . هنا علاقات الثقة مابين أثنين Domain تجعل الـ Domain الأول أن يثق بخدمة التحقيق authentication تابعة للـ Domain الثاني وان يستخدم عناصر الـ Domain الثاني من أجل عملية تأمين الموارد . وهي عبارة عن أرتبط منطقي ينشأ مابين الـ Domains من أجل أن يتخطي عملية التحقيق ولا تكون منحصرة على Domain واحد.

خصائص علاقات الثقة :

علاقات الثقة مابين أكثر من Domain ممكن أن توصف عن طريق ثلاث خصائص من خصائص الثقة :

- **الاتجاه Direction :**

علاقة الثقة ممكن أن تكون اتجاه واحد One-Way أو في الاتجاهين Two-Way . في علاقة الاتجاه الواحد مثل التي في الصورة التالية:

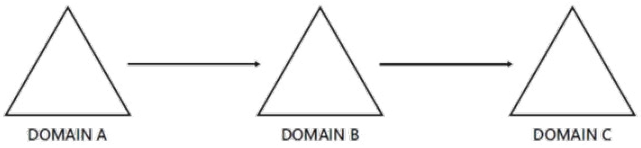


المستخدمين في الـ Domain الموثوق به (Trusted Domain) ممكن ان نسند له ونعطيه صلاحيات الدخول لموارد في الـ Domain الواثق به (Trusting Domain) ، لكن المستخدمين في (Trusting Domain) لا يمكن ان نسند لهم صلاحيات لموارد في الـ (Trusted Domain) . في أغلب الأحيان ممكن أن تُنشئ ثقة من اتجاه واحد ثانية في الاتجاه المعاكس لنعمل ثقة من نوع الاتجاهين .

على سبيل المثال ، ممكن أن تنشئ علاقة ثقة ثانية والتي هي أن Domain B يثق بـ Domain A . وبعض علاقات الثقة افتراضيا By Default تكون علاقة ثقة في الاتجاهين Two-Way . وفي هذه الحالة كلا الـ Domains يثقوا بالعناصر والـ Objects الموجودة في أي Domain .

- **الانتقالية Transitivity :**

بعض العلاقات لا تكون انتقالية والبعض يكون انتقالي . في الصورة التالية Domain A يثق بـ Domain B و Domain B يثق بـ Domain C . أذا كانت العلاقة انتقالية ، أذاً Domain A يثق أيضا بـ Domain C . لكن اذا كانت ليست انتقالية في هذه الحالة Domain A لا يثق بـ Domain C .



- **التلقائي و اليدوي Automatic or Manual :**

بعض علاقات الثقة تُنشئ تلقائياً . والبعض يجب مدير الشبكة أن ينشئها يدوياً.

كيف تعمل علاقات الثقة :

في نفس الـ Forest كل الـ Domains يثقوا بعضهم البعض ، وهذا بسبب أن أول domain في كل Tree في الـ forest يثق بأول Domain في كل Tree في نفس الـ Forest ، وكل Child يثق بالأب تبعه Parent Domain . كل علاقات الثقة التي تنشئ تلقائياً يجب أن لا تمسح أبداً وهي أيضا من النوع الانتقالي و من الاتجاهين . والنتيجة تكون ان كل الـ Domains يثقوا بعضهم وعملية التحقق من أسم المستخدم وكلمة السر ممكن أن تكون على أي Domain في الـ forest . وأيضا المستخدمين والمجموعات من نوع الـ Global من أي domain في الـ Forest ممكن أن تضاف إلى مجموعة من النوع domain Local وممكن ان نسند لها صلاحيات وممكن ان نحطها في الـ ACLs تبع أي ملف أو مجلد أو طابعة في أي domain أخر في نفس الـ Forest . لكن علاقات الثقة في forest آخر أو Domain آخر خارج الـ Forest يجب ان تُنشئ يدوياً .

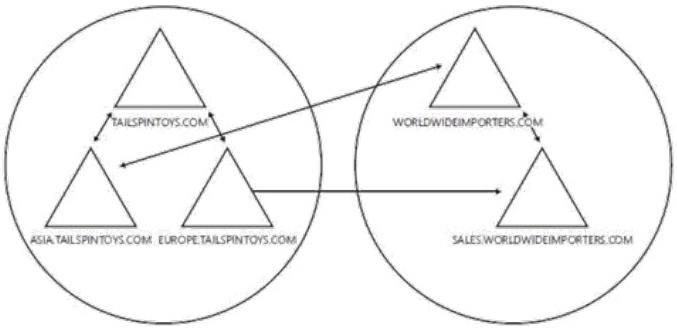
وللتعرف على أنواع علاقات الثقة داخل الـ forest او خارجها تابع معي الأسطر القادمة .

أنواع الثقة (Trust):

هناك أربعة أنواع من الـ Trusts يجب ان نعملها يدويا :

الأولى - External Trusts - :

عندما تحتاج انك تشتغل على Domain والـ Domain ده كان ليس تبع الـ Forest حقك ، أنت أذا تحتاج إلى إنشاء External Trusts ، الـ External Trusts هو علاقة ثقة مابين Domain في حقك الـ Forest و Domain ثاني مش موجود بحقك الـ Forest على سبيل المثال الصورة التالية:

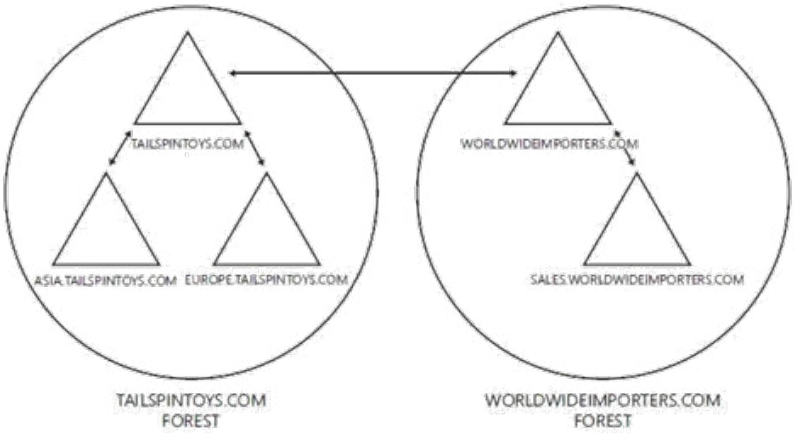


في الصورة تلاحظ هناك ثقة من جهة وحدة مابين Domain الـ sales.worldwideimporters.com و Domain الـ europe.tailspintoys.com ، طيب الـ Europe يثق بالـ Sales أذا المستخدمين في الـ Sales ممكن يدخلوا على الكمبيوترات في الـ Europe Domain أو يدخلوا على موارد مثل الطابعات والملفات في Domain الـ Europe .

وكمان لو نلاحظ في الصورة يظهر لنا ثقة من الاتجاهين مابين الـ worldwideimporters.com و Domain الـ asia.tailspintoys.com . هنا يعني ان المستخدمين من كلا Domains ممكن ان يدخلوا على موارد في أي Domain لهذا أطلقوا عليها أسم ثقة من الاتجاهين . وهنا نقول أن كل الـ External Trusts يطلقوا عليهم non-transitive يعني غير انتقاليين بمعنى مش ان الـ worldwideimporters.com يثق بالـ sales.worldwideimporters.com كما في الصورة والـ worldwideimporters.com يثق بالـ asia.tailspintoys.com مش معناها أن الـ asia.tailspintoys.com يثق بالـ sales.worldwideimporters.com هذه معنى non-transitive ..

النوع الثاني - الـ Forest Trust - :

عندما تحتاج إلى أن تضم أو تتشارك الموارد مابين شركتان منفصلتان وكل وحدة منهم لها الـ Forest حقها ، ممكن تأخذ بعين الاعتبار أو تعمل ما بينهم Forest Trust . الـ Forest Trust عبارة عن ثقة من اتجاه واحد أو من اتجاهين وتكون علاقة ثقة انتقاليه transitive مابين أول Domain في الـ Forest الأولى او كما يسمى بالـ Forest Root Domain وأول Domain في الـ Forest الثانية والصورة توضح أكثر .



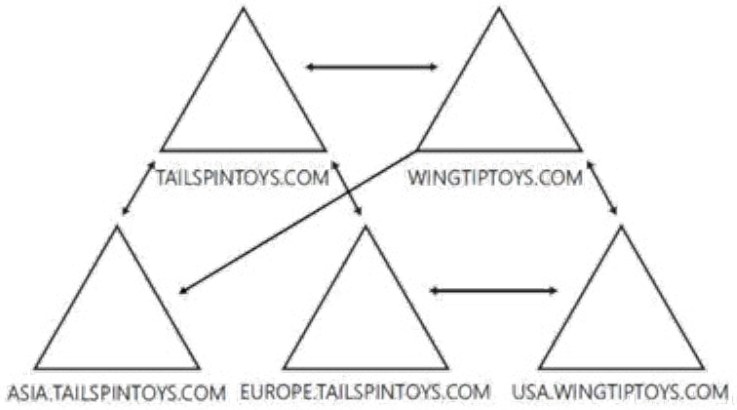
وهي عبارة عن علاقة ثقة مابين الـ Forest حق الـ tailspintoys.com والـ Forest حق الـ worldwideimporters. com . وقصد هنا بالانتقالية transitive أنه لما forest تثق بـ Forest ثانية يعني كل الـ Domains الفرعية من الـ Forest تثق بالـ Forest الثانية والعكس صحيح ، وهذا الكلام عكس الثقة الي من النوع External Trust كما عرفنا في تلميحه سابقة .

وفي هذا النوع من الثقة يسمح لنا من أن المستخدم يعمل authentication في أي Domain وعن طريق أي Domain أخر في أي من وحدة من الـ forests ، طبعا الفقرة دي الي فوق على افتراض أن الثقة كانت بالاتجاهين Two-way Trust.

طيب هذا النوع من الثقة بكل بساطة ممكن نعمله ونديره على غرار أننا نعمل ثقة مابين كل الـ Domains في الـ forest زي الـ External ، طبعا ده النوع نعمله عندما تكون مثلا شركة قامت بشراء شركة أخرى أو تريد أن تشارك الموارد ما بينهم أو حتى عندما تكون الشركة كبيرة وفيها أكثر من Forest ..

النوع الثالث - Shortcut Trust - :

ومن أسمة يعني ثقة بس مختصرة ، لنفترض المثال التالي لو مثلا عملنا ثقة مابين Two Forest وكان في كل Forest في كدا Child وكل Child في منه Child ثاني طيب في دي الحالة لو الـ Child الأخير إلي في الـ Forest الأولى يشتي يروح يكلم مثلا سيرفر في أخر Child Domain في الـ Forest الثانية في دي الحالة المسار سيكون من الأسفل إلى الأعلى بمعني أخر Child يذهب يكلم الي فوقة والي فوقه يذهب يكلم الـ Forest Root Domain وهو بعدين بذهب يكلم الـ Forest Root Domain حق الـ Forest الثانية وهو بيعمل العملية العكسية يعني سيكون إلى الأسفل بيسأل الـ Child والـ Child بيودي للـ Child إلي تحته وهنا بعرف ده الـ Child Domain أنه السيرفر موجود عنده فا بيعمل للمستخدم Authentication ويسمح له بالدخول ، طيب كل ده يسبب بطئ في أداء الدخول للموارد .. طيب لكن مع الـ Shortcut Trust بصراحة هو أتعمل عشان يحل لنا دي المشاكل عن طريق إنشاء علاقة ثقة مباشرة مابين الـ Child Domains في مسار الثقة مابين الـ Forests والصورة توضح ذلك ..



طيب الـ Shortcut Trust يسرع عملية الـ Authentication مابين الـ Childs Domain في أكثر من Forest عن طريق انه لا يسلك نفس الطريقة الي فوق ويذهب من Domain إلى الـ Domain الذي أعلى منه وهكذا وفي هذه الحالة يتحسن الأداء إلى حدا ما ..

والـ Shortcut Trust ممكن أن يكون One-Way أو Two-Way وعرفنا ماذا يعني بهم في السابقة ، وفي أي حالة من هذه الحالات أكيد الثقة بتكون انتقالية Transitive. وكما نلاحظ في الصورة هناك One-Way Shortcut Trust موجودة ، حيث أن wingtiptoys.com يثق بي asia.tailspintoys.com . طيب عندما مستخدم من الـ asia.tailspintoys.com يدخل على مثلا سيرفر موجود في wingtiptoys.com أو يطلب أي مورد من الموارد الموجودة في wingtiptoys.com الطلب ممكن أن يأخذ المسار مباشرة إلى الـ Domain الذي هو wingtiptoys.com دون أخذ المسار تصاعديا كما في السابق وهنا العكس غير صحيح لأنه One-Way Shortcut Trust وهو عندما مستخدم في wingtiptoys.com يدخل على سيرفر موجود في الـ asia.tailspintoys.com الطلب يأخذ المسار تصاعديا كما في السابق لانة كما عرفنا في الـ Forest Trust أنها Transitive ..

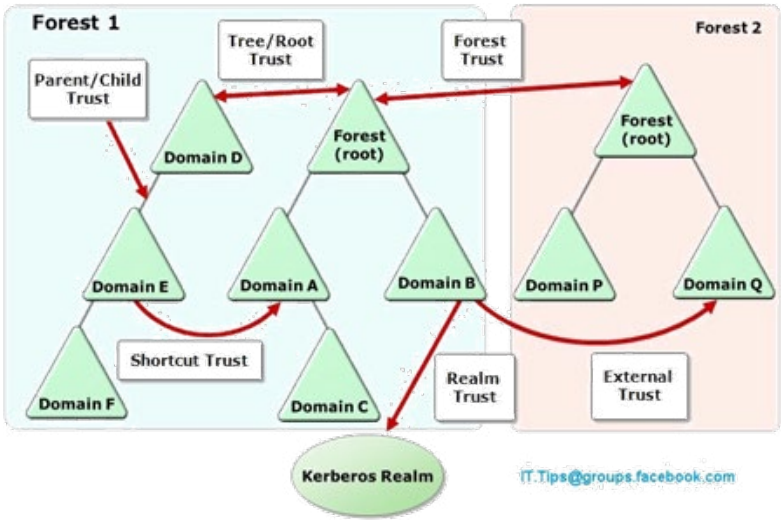
وفي الصورة معانا أيضا Two-Way Shortcut Trust مابين usa.wingtiptoys.com والـ Domain الذي هو europe.tailspintoys.com يعني المستخدمين في كلا الـ Domains ممكن أن يعملهم authenticated ويعملوا طلب للموارد من الكمبيوترات في الـ Domain الأخر ، والـ Shortcut Trust هو الي يستخدم ..

النوع الرابع - Realm Trust - :

وهذا النوع غير مستخدم كثير ونعمله لما نشتي نعمل تنفيذ وتوافقية في خدمة الأمن أو برتوكول الأمن (Kerberos v5) مابين أكثر من Platform ، يعني تستطيع تعمل Realm Trust مابين الـ Domain (Windows Domain) و جهاز UNIX محمل علية خدمة الـ Authentication إلي هي برتوكول الـ (Kerberos v5) . طيب ده النوع عبارة عن One-Way Trust لكن تقدر تعمل One-way في كلا الاتجاهات وبا يصبح معانا Two-Way Trust . والحاجة الثاني انه افتراضيا (By Default) يكون غير أنتقالي Non-Transitive لكن ممكن تخليه Transitive .

طيب اذا كان معانا جهاز نثق فيه ومحملين علية الـ (Kerberos v5) وكان مش من مايكروسوفت non-Windows اذا هذا النوع يثق بكل حاجات الأمن في حقك الـ Domain يعني المستخدمين في جهة الجهاز الي هو non-Windows ممكن يسمح لهم الدخول إلى الموارد في حقك الـ Domain ، لكن العملية غير مباشرة .

طيب وفي هذا النوع أيضا ممكن أن تعمل Map لمستخدم من مستخدمين الويندوز على ويندوز Domain ممكن تسنده لنظير (Kerberos v5) على جهاز non-Windows ، بمعنى انه السماح لحساب مستخدم في الويندوز نحطه على جهاز non-Windows ومن شان نتلاعب فيه ولأغراض إدارية على سبيل المثال group policy, home directory, etc.)) .. طبعا هذا النوع لا يطول الكلام علية لقلة استخدامه .. ولننظر على الصورة التالية والتي تشرح لنا كل أنواع الـ Trusts حتى معا أنواع لم يتم ذكرها سابقا وهي Tree/Root Trust و الـ Parent/Child Trust لم يتم شرحها لانها تكون موجود By Default وتسمى Built in Trust ..



ونلتقي في سلسلة جديدة أن شاء الله .. تحياتي لكم ..

أيهم أفضل CCNP Sec أم CEH !!

سؤال طالما يصلنى على البريد ألا وهو أيهم أفضل هذه الشهادة أم تلك ؟ وأغلب السائلين يقتصر سؤالهم على شهادتين فقط ولا أعلم السبب فى ذلك وهما شهادة CCNP Security التى تقدمها شركة سيسكو فى مجال أمن الشبكات ,وشهادة CEH المقدمة من EC-Council لهذا السبب أحببت ان يكون هذا السؤال هو عنوان مقالى لهذا العدد .

فى البداية هل أنت مؤهل لطرح هذا السؤال ؟

قبل أن تفكر فى طرح أى سؤال فكر قبلها هل ستستفيد من الإجابة التى ستكون رد على سؤالك ,ما أقصده هنا هو أن السائل فى أغلب الأحوال لا يكون عنده الحد الأدنى من المعلومات التى ستمكنه من فهم الفروقات بين الشهادتين, فإن كان السائل مازال ببداية طريقة فى دراسة حماية الشبكات وأمن المعلومات فكيف سيستطيع فهم محتويات شهادة مقدمة لفئة المتقدمين والمحترفين, عندها يكون ردى كتالى :

قبل أى شىء يجب عليك أن تكون ملم بأساسيات الشبكات وأمن المعلومات ولا تظن أن هذه الأساسيات بسيطة بل هى أصعب الخطوات لأنها أساس ستنبنى عليه ما ستتعلمه فيما بعد وللحصول على هذه الأساسيات قم بدراسة الشهادات التالية:

1 - N+من شركة كومبتيا لأنها ستعلمك ألف باء شبكات .
2 - CCNA ستعطيك المزيد من التفاصيل بالاضافة إلى البداية فى اعداد أجهزة الشبكة بنفسك .
3 - بعد ذلك يمكنك دارسة اما شهادة CCNA Sec أو Security+ للحصول على أساسيات الأمن والحماية والتعرف على مصطلحات هذا المجال مما يسمح لك بالتعمق أكثر ومعرفة المزيد .

هذا رد جاهز عندى امرره إلى أى شخص يوجه إلى أى سؤال متعلق بشهادات متقدمة قبل أن يبدأ بالأساسيات ,أما فى حال كنت ملم بكل هذه الأساسيات ولا يناسبك هذا الرد فتابع معى .

قبل أن تسأل تأكد من أن سؤالك منطقى وسليم

نفتقر فى مواقعنا ومنتدياتنا إلى الطريقة الصحيحة فى طرح الأسئلة التى تساعد من يقوم بالرد وتوفر عليه الكثير من العناء لفهم السؤال, فاذا وجهت لك هذا السؤال أيهم أفضل الروتر أم السويتش ؟ بالطبع سؤال غير منطقى لأنه يقارن بين جهازين مختلفين لكل منهم مهام مختلفة عن الاخر فلماذا أتعب نفسى لمعرفة الأفضل بينهم, نفس المبدأ بالنسبة لشهادة مثل CCNP Security وأخرى مثل CEH, فاذا قمت ببعض البحث فى محتوى كل شهادة ستجد أن هناك شىء يسمى بأمن وحماية الشبكات Network Security و أمن المعلومات Information Security, فهناك مفهوم سائد عند أغلب المبتدئين فى هذا المجال وهو أن كلها شهادات هاكنج طالما تتعلق بالأمن والحماية وبمجرد دراستها ستتمكن من الإختراق ,وهذا مفهوم خاطىء وستتضح لك الحقيقة عند التعمق أكثر والوصول إلى مستويات أعلى .

أمن الشبكات وأمن المعلومات ليسا وجهان لعملة واحدة

كما قلت فالمجالان مختلفان ففى المجال الأول وهو أمن الشبكات ستجد أهم المواضيع تتعلق بالبنية التحتية للشبكة وأجهزتها المختلفة التى سيكون همك الشاغل هو التأكد من استمرار عملها وعدم توقفها بسبب أى هجوم قد يستهدف هذه الأجهزة, ولأن معظم هذه الأجهزة يقتصر عملها على أول أربع طبقات من OSI Model فبالتبعية سيقتصر عملك أنت أيضا على هذه الطبقات الأربعة, مما يعنى أنه قد لا يلزمك التعمق فى تفاصيل الطبقة الأولى Application Layer والتعرف على معمارية الهجمات التى تحدث فى مستوى هذه الطبقة وهذا لعدة أسباب أولها أنها ستحتاج منك إلى خلفية برمجية قوية بالاضافة إلى أنها قد تكون من إختصاص شخص أخر كمدير الأنظمة الذى يعرف كيف يؤمن سيرفراته على هذه الطبقة, صحيح أنك كمسئول عن أمن الشبكة يمكنك منع هذه الهجمات من البداية ولكن هناك أشياء أهم ستحتل قائمة اولوياتك .

الفرق بين Network security و Information security

أمن الشبكات هو قيامك بالاعدادات الأساسية لأجهزة الشبكة لحمايتها بالاضافة إلى التعامل مع أجهزة الحماية الخاصة مثل الجدران النارية وسيرفرات التحكم بالوصول والمحتثات, فكلها أجهزة يجب أن تتقن التعامل معها اذا كان هدفك أن تكون مهندس متخصص بأمن الشبكات, بينما أمن المعلومات هو تخصص اخر يهتم بجوانب مختلفة فى عالم الحماية ويفضل أن تبدأ تخصصك فى هذا الفرع باتقان لغة برمجة قوية وبعد ذلك تبدأ بالتعرف على الأدوات التى يتم استخدامها فى تنفيذ الهجمات ومنهجية شنها حتى تستطيع التصدى لها فيما بعد .

شهادات متعلقة بأمن الشبكات

CCNA Sec هى شهادة ستساعدك فى التعرف على أساسيات هذا المجال من وجهة نظر شركة سيسكو وفلسفتها الخاصة فى الحماية .

CCNP Sec هى مستوى أعلى من الشهادة السابقة تجعلك محترف فى تطبيق حلول سيسكو الأمنية التى قد تحصن شبكتك ضد أى تهديدات .

CCIE Sec هى الشهادة الأعلى التى تقدمها سيسكو لشخص يمكن ان نطلق عليه لقب خبير فى تطبيق حلولها الأمنية والتعامل مع أجهزتها .
JNCIS-SEC - JNCIP-SEC - JNCIE-SEC

ثلاثة شهادات تقدمهم شركة جونيبر للتعريف بالحلول التى تطرحها هذه الشركة فى مجال حماية الشبكات ,وهى الأخرى تقدم شهاداتها بشكل هرمى قاعدته المبتدىء وقمته المحترف والخبير .

Fortinet Certification تقدم هذه الشركة حزمة من الشهادات المتخصصة فى حماية الشبكات, تتميز شهادتها بالتخصصية حيث تجد شهادة منفصلة للجدران النارية واخرى للمحثثات وهكذا

شهادت متعلقة بأمن المعلومات

بما أن هناك تفرعات كثيرة هنا فلن أطرح شهادات بل سأكتفى بأسماء الشركات التى تقدم أشهر الشهادات ومنها :

EC-Council تقدم هذه الشركة الشهادة الشهيرة CEH الخاصة بالاختراق الأخلاقى كما يطلق عليه ,وعكس ما هو شائع فهذه الشهادة ما هى الا خطوة اولى بهذا الطريق ,حيث ستتعرف فيها على كم هائل من أدوات اختبار الاختراق .

Offensive-Security وهى لمن لا يعلم مطورة توزيعة اللينكس الشهيرة باك تراك ,ولها العديد من الشهادات التى توازى شهادات ec-council اذا لم تتفوق عليها .

Sans وتقدم أقوى الشهادات فى مجال أمن المعلومات ,وفخر لكل شخص ان يكون من الحاصلين على أحد شهادتها فهى اشبه بالحزام الأسود فى هذا المجال وسيكون هناك مقالات قادمة حول هذه الشهادات .

هكذا أكون قد انتهيت من مقالى لهذا العدد الذى أتمنى أن أكون قد قدمت فيه معلومة جديدة ,وارحب بأى استفسار أو سؤال متعلق بهذا الموضوع .


Magazine
NetworkSet